

Singapore Management University

Institutional Knowledge at Singapore Management University

Dissertations and Theses Collection (Open Access)

Dissertations and Theses

6-2021

Culture and cyber security: How cultural tightness-looseness moderates the effects of threat and coping appraisals on mobile cyber hygiene

Kok Wei HOE
Singapore Management University

Follow this and additional works at: https://ink.library.smu.edu.sg/etd_coll



Part of the [Business Administration, Management, and Operations Commons](#), and the [Organizational Behavior and Theory Commons](#)

Citation

HOE, Kok Wei. Culture and cyber security: How cultural tightness-looseness moderates the effects of threat and coping appraisals on mobile cyber hygiene. (2021). 1-121.

Available at: https://ink.library.smu.edu.sg/etd_coll/357

This PhD Dissertation is brought to you for free and open access by the Dissertations and Theses at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Dissertations and Theses Collection (Open Access) by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

**CULTURE AND CYBER SECURITY: HOW CULTURAL
TIGHTNESS-LOOSENESS MODERATES THE EFFECTS OF
THREAT AND COPING APPRAISALS ON MOBILE CYBER
HYGIENE**

HOE KOK WEI

SINGAPORE MANAGEMENT UNIVERSITY

2021

**CULTURE AND CYBER SECURITY: HOW CULTURAL
TIGHTNESS-LOOSENESS MODERATES THE EFFECTS OF
THREAT AND COPING APPRAISALS ON MOBILE CYBER
HYGIENE**

HOE KOK WEI

Submitted to Lee Kong Chian School in partial fulfilment of the requirements
for the Degree of Doctor of Business Administration

Thesis Committee

Dr. Roy CHUA (Supervisor/Chair)

Associate Professor of Organizational Behavior and Human Resources
Singapore Management University

Dr. Onur BOLABATLI

Associate Professor of Operations Management
Singapore Management University

Dr. KE Ping Fan

Assistant Professor of Information System
Singapore Management University

Singapore Management University 2021

Copyright (2021) HOE Kok Wei

I hereby declare that this Doctor of Business Administration dissertation is my original work and it has been written by me in its entirety.

I have duly acknowledged all the sources of information which have been used in this dissertation.

This Doctor of Business Administration dissertation has also not been submitted for any degree in any university previously.

A handwritten signature in black ink, consisting of a large, stylized loop followed by the name 'Kok Wei' in a cursive script, ending with a horizontal line and a dot.

HOE Kok Wei

14 Jun 2021

ABSTRACT

With increasing adoption of smartphone for mobile-commerce and increasing incidents of cyber breaches, it is timely to investigate how the weakest link in this security chain, human, can be strengthened. To date, there has been a gap in research examining the impact of culture on protection motivation. Most extant research focus on technological, organizational and behavioral factors affecting protection motivation. In this study, I develop a model integrating Theory of Cultural Tightness-Looseness and Protective Motivation Theory to investigate how cultural norms, define as shared expectations and rules that guide behavior of people within social groups, affect a person's intentions to adopt protective measures on their devices. Using the Cultural Tightness-Looseness theory, I hypothesize that cultural norms provide important indications to an individual's evaluations of threat and coping strategies. My study weaves extant research adopting Protection Motivation Theory to investigate information security behaviors, to determine how social influences of the environment (as explained by theory of Cultural Tightness-Looseness) and psychology of the individual (as explained by Protection Motivation Theory) interact and determine the eventual individual security behavior. The study is conducted over 31 provinces of China, and expands extant research beyond desktop computers to smartphones, and organization setting to the personal phone user, where it is up to the individual motivation and cultural environment to be aware of cyber threats, understand cyber risk, and take protective actions against cyber breaches. The findings of this study contributes towards developing more comprehensive and systematic measures

and messaging to motivate individual to adopt protective measures on their devices.

TABLE OF CONTENTS

1	INTRODUCTION.....	1
2	PURPOSE OF THE STUDY	3
2.1	Focus of Extant Research.....	3
2.2	The Prevalence of the Mobile Phone and the Rise of China	4
3	CONTRIBUTION.....	6
4	THEORETICAL DEVELOPMENT	8
5	LITERATURE REVIEW	9
5.1	Cyber Hygiene	9
5.2	General Deterrence Theory	10
5.2.1	Severity of Punishment	11
5.2.2	Certainty of Punishment.....	11
5.2.3	Celerity of Punishment.....	11
5.3	Theory of Planned Behavior	12
5.3.1	Attitude	12
5.3.2	Subjective norms.....	12
5.3.3	Perceived behavioral control.....	12
5.4	Protection Motivation Theory	12
5.4.1	Perceived Vulnerability.....	13
5.4.2	Perceived Severity.....	13
5.4.3	Self-Efficacy	13
5.4.4	Response Efficacy.....	13
5.4.5	Response Cost	14
5.5	Cultural Tightness-Looseness	15
6	RESEARCH QUESTION	19
7	RESEARCH MODEL	20
8	HYPOTHESES	22

8.1	Main effects	22
8.1.1	Threat Appraisal.....	24
8.1.2	Coping Appraisal	25
8.2	Moderating Effects	28
8.3	Intentions and Behaviors	34
8.4	Summary of Hypotheses and Research Model	36
9	METHODOLOGY	37
9.1	Sample and Data Collection.....	37
9.2	Measures	37
9.2.1	Independent Variables (Predictors).....	37
9.2.2	Dependent Variables (Response variables).....	37
9.2.3	Moderators	38
9.2.4	Measures of Protection Motivation.....	38
9.2.5	Measures of Mobile Cyber Hygiene-B (MCH-B).....	39
9.2.6	Measures of Personality.....	40
9.2.7	Measures of Regulatory Focus.....	40
9.3	Data Screening.....	40
10	RESULTS	42
10.1	Reliability.....	42
10.2	Approach.....	42
10.3	Correlation	43
10.4	Fixed or Random Effects	44
10.5	Control Variables (Demographics).....	44
10.6	Main Effects with Independent Variables.....	44
10.7	Main Effects with Independent Variables and Moderators	45
10.8	Effects of Intentions on Behavior	46
10.9	Main Effects and Moderations on Mobile Cyber Hygiene Behaviors.....	46

10.10	Full Model Analysis using Path Analysis (Moderated Mediation).....	47
11	Hypotheses Testing	48
11.1	Hypothesis 1 – Cultural Tightness-Looseness has a positive effect on Mobile Cyber Hygiene Intentions	48
11.2	Hypothesis 2 – Perceived Security Vulnerability has a positive effect on Mobile Cyber Hygiene Intentions.....	48
11.3	Hypothesis 3 – Perceived Security Severity has a positive effect on Mobile Cyber Hygiene Intentions	49
11.4	Hypothesis 4 – Security Self-Efficacy has a positive effect on Mobile Cyber Hygiene Intentions	49
11.5	Hypothesis 5 – Response Efficacy has a positive effect on Mobile Cyber Hygiene Intentions	49
11.6	Hypothesis 6 – Response Cost has a negative effect on Mobile Cyber Hygiene Intentions	49
11.7	Hypothesis 7 – The tighter the culture, the stronger is the positive effect of Perceived Security Vulnerabilities on Mobile Cyber Hygiene Intentions.	50
11.8	Hypothesis 8 – The tighter the culture, the stronger is the positive effect of Perceived Security Severity on Mobile Cyber Hygiene Intentions	50
11.9	Hypothesis 9 – The tighter the culture, the weaker is the positive effect of Security Self-Efficacy on Mobile Cyber Hygiene Intentions	51
11.10	Hypothesis 10 – The tighter the culture, the stronger is the positive effect of the Response Efficacy on Mobile Cyber Hygiene Intentions	51
11.11	Hypothesis 11a/11b – The negative effects of Response Cost on Mobile Cyber Hygiene Intentions are weaker/stronger in a tight culture when compared to a loos culture.....	51
11.12	Hypothesis 12 – Mobile Cyber Hygiene Intentions has positive effect on Mobile Cyber Hygiene Behaviors	52
12	SUPPLEMENTARY ANALYSES	53
13	DISCUSSION	57
13.1	Main Effects.....	57
13.2	Moderator’s Effects	59
14	THEORETICAL CONTRIBUTION	62
15	PRACTICAL IMPLICATIONS.....	63
16	LIMITATIONS	65

17	CONCLUSIONS	67
18	REFERENCES.....	68

LIST OF TABLES

Table 1 Culturally Tight vs Culturally Loose	86
Table 2 Summary of Hypotheses	88
Table 3 Respondent's Demographics	89
Table 4 Cronbach's Alpha.....	90
Table 5 Correlation	91
Table 6 Regression with Control Variables	92
Table 7 Regression with Predictors	93
Table 8 Regression with Predictors and Moderators	94
Table 9 Regression of Mobile Cyber Hygiene Intentions on Mobile Cyber Hygiene Behaviors.....	95
Table 10 Regression with Mobile Cyber Hygiene Behaviors as Dependent Variable.....	96
Table 11 Path Analysis (Intention)	97
Table 12 Path Analysis (Behaviors)	98
Table 13 Results of Hypotheses Testing.....	99
Table 14 Comparison of Regression vs Path Analysis (Intentions)	101
Table 15 Comparison of Regression vs Path Analysis (Behaviors)	102
Table 16 Supplementary Analysis with Regulatory Focus Predictors.....	103
Table 17 Supplementary Analysis with Big 5 Personality Traits	104

LIST OF FIGURES

Figure 1 Research Model	105
Figure 2 Research Model and Hypotheses.....	106
Figure 3 Margin Plot of Cultural Tightness Moderated with Perceived Security Severity	107
Figure 4 Margin Plot of Cultural Tightness moderated with Response Cost	108
Figure 5 Regression Results.....	109

ACKNOWLEDGMENTS

First and foremost, I would like to express my extreme gratitude to my supervisor, A/P Roy CHUA, for the guidance and support throughout this last phase of the DBA journey. His candid remarks guided me tremendously. When I hit walls and felt burnt out trying to discern the data and connect the dots, his pointers and encouragement helps me to stay afloat and focused.

I am also grateful for the valuable feedback and suggestion from the rest of my dissertation committee, A/P Prof KE and A/P Prof Onur. Your remarks help me to sharpen the approach and strengthen the outcome.

I would also like to thank the wonderful staff of the LKC School of Business for their help in the whole DBA journey. Special mention to Louis and Vivian for their hands-on support.

To all my DBA course mates and RA, thanks for the encouragement and support throughout the journey. My journey in this course is greatly enhanced by the interaction with all of you.

Finally, special thanks to my family for their immeasurable patience, especially my wife Priscilla, for standing-in to coach the kids while I crunch the data in my man-cave.

This dissertation was written with support from the
ASEAN Business Research Initiative (ABRI) Grant #G17C20411

1 INTRODUCTION

Many users lack the expertise to ensure safe computing, defined as a set of practices that protect your computing devices from harm. Most people also tend to frame cyber vulnerabilities as a technological problem, failing to perceive that most cybersecurity vulnerabilities are often the result of human behavior. In a typical security chain comprising internet security, cloud security, network security, medium security and end point security, many people fail to realize that the human at the last mile (end point security) is the weakest and most vulnerable point of the whole security chain. For example, social engineering scams, the most familiar cyber-attack approach, is based on targeting and manipulating a potential victim's human weaknesses. Moreover, the attitude and behaviors of human in this security chain is significantly determined by his or her culture, which is the tacit order of a society (Groysberg et al., 2018). In a culture where the norms are avoiding mistakes due to strong collective culture, an individual being compromised by social engineering scam might withhold that mistake for fear of being punished. This will hinder the incident response and subsequent investigation of the cyber-attacks. Besides, the plethora of technological solutions for strengthening the security chain would not prevent an individual from accidentally clicking a link downloading malware into the network. The security chain remains as vulnerable as its weakest link. Coupled with increasing use of mobile devices to access essential services (e.g., banking, online shopping, government services, etc.) on the Internet, it is paramount that we study the human factors that lead to cyber vulnerabilities.

One approach to strengthening this security chain is to increase awareness and training, which includes both the security mechanism they can use to protect information (usually technology centric), as well as increasing their awareness of the potential threats to the security chain. In addition, such training must be extended beyond the organization settings into the personal environment, and beyond the desktops and networks onto the ubiquitous mobile phone. While failure to adopt proper security practices in an organization might result in financial losses and increased downtime on the network and computers, home users face identity theft which results not only in financial losses, but also loss of privacy.

2 PURPOSE OF THE STUDY

2.1 FOCUS OF EXTANT RESEARCH

Extant research on the human component within information technology security chain is relatively few. The research often revolves around information security rather than cyber security. While the former comprises confidentiality, integrity and availability of information (also known as the CIA triangle model), the latter has additional dimensions including humans in their personal capacity and society at large. These individuals can be directly harmed or affected by breaches in cyber security (Von Solms & Van Niekerk, 2013). For example, cyber bullying where technology is used to cause embarrassment, involve harassment and inflict psychological harm (Martin & Rice, 2011). Earlier research also tends to focus on the organization, where there are explicit information system security policies, dedicated training to educate the employees on the need for compliance, and dedicated support staff to support the employees should a cyber-attack take place. In a personal setting, where such studies are few and far between, it is up to the individual to be aware and understand potential security threats to his or her home computer system and acquire the necessary knowledge and technical skills sets to respond to such threats.

There is also limited research on the social factors influencing people to perform certain behaviors to protect against information security threats. Most research inspect the direct relationship between end-user security technical knowledge, their attitudes and beliefs and their compliance with information system security policies (ISSP) as predictor of information security behavior. They do not consider the impact of social influences of the environment and the

psychology of the individual (individual security behavior) on the eventual security intentions and behavior. Research on the social factors affecting the security behaviors of human in the information security chain on mobile devices is usually based on organizational or personal computers.

Lastly, most extant research on behavioral information security rely on intention-based models as a proxy for actual behavior, such as Theory of Reason Actions (Vinet & Zhedanov, 2011), Theory of Planned Behavior (Ajzen, 1985) and Protection Motivation Theory (Rogers, 1975). These intention-based theories assume that intention is a strong predictor of behaviors. Unfortunately, it is not uncommon to observe individuals behaving contrary to their intentions (Ajzen et al., 2004).

2.2 THE PREVALENCE OF THE MOBILE PHONE AND THE RISE OF CHINA

Mobile phones are increasingly becoming the medium to exchange all kinds of information. Their portability and affordability overcome the traditional barriers to internet, expanding access to even low-income and rural population. The increased usage of mobile phones also introduces new risk as it is more ubiquitous, where most people will likely see their first message. However, its smaller screens and limited display of detailed information also increases the likelihood of phishing success. For example, an email opened in the mobile phone might only display the sender's name unless you expand the header information. However, expanding information on the small screen of the mobile, also has a higher likelihood of accidentally clicking action-oriented buttons which might introduce malware into the devices. Additionally, the

increased use of mobile devices also render it more attractive for attackers to target mobile user than traditional desktop users (*8 Mobile Security Threats You Should Take Seriously in 2020 / CSO Online*, n.d.).

For a study involving mobile phone usage, China is undoubtedly the ideal destination. In March 2020, the China Internet Network Information Centre reported that the total number of Chinese internet users was 904 million, with 897 million (99.3%) accessing the internet via smartphones (*China Internet Network Information Center (CNNIC)*, n.d.). This makes China the world's biggest mobile market in terms of subscriber base and the fastest growing in the history of telecommunications. With this critical mass of mobile users, China is emerging as a global capital of m-commerce (mobile commerce), an extension of e-commerce where business transactions are conducted in a mobile environment using mobile devices.

3 CONTRIBUTION

This research extends existing security behavioral studies on information and/or cyber security to draw attention to how cultural differences, defined by the strength of their social norms and tolerance toward deviant behavior (Gelfand et al., 2006), moderates the effects of cyber hygiene behaviors predictors, which is defined as the set of practices that prevent negative impact. It examines how cultural tightness and looseness – the degree to which a society is characterized by rules and norms and the extent to which people are punished or sanctioned when they deviate from these rules and norms – influences the effectiveness of predictors of cyber hygiene behaviors. In a tight culture, social norms are the primary driver of behaviors and people rely more on collective thinking and homogeneity of thought. In contrast, loose culture celebrates self-efficacy and challenges to establishment. For example, in Japan, a traditional and culturally tight society, children are taught to abide by rules from a very young age; whereas, in a culturally loose society like America, parents encourage exploration and rarely impose punishments on their children. Such socialization (narrow in a tight society and broad in a loose society) will in turn affect how the kids behave when they grow up.

To determine the security behavior of mobile phone users, I draw on the Protection Motivation Theory (Rogers, 1975) which has been widely adopted for understanding security behavior. Protection Motivation Theory suggests that when an individual is faced with a threatening event, the individual's behavior in response to that threatening event is motivated by threat and coping appraisal. Threat appraisal refers to the perceived severity of the impact and the likelihood of the threat occurring while coping appraisal refers to the individual's ability

to engage in a protective behavior in a cost-effective manner. Protection Motivation Theory has since been applied successfully to a broad range of threat related studies. Since my study is about determining how people respond to cyber threats, and computer security has often been referred to it as computer health (Dave Kearns, 2006), I expect this theory to display similar effects when applied to the study of cyber security protective behaviors. Collectively, I posit that the tighter the culture, the stronger the tendency to punish deviant behavior, the stronger the effects of threat appraisal (the determination of how severe a given threat is and how vulnerable he/she is to the threat) on mobile cyber hygiene as people will adopt measures to avoid punishment. For the same reason, tighter culture will also strengthen the effects of coping appraisal (the determination of how well the coping mechanism can be performed and how effective the coping mechanism is at providing protection from the threat) on mobile cyber hygiene.

This study will also be mobile phone centric and based on personal users, in contrast to the numerous similar studies which are personal computer centric and based on employees working within an organization.

Additionally, this study will also be conducted in China, which has the largest number of smartphone users in the world, over 897 million users. Covering most, if not all, of the provinces, this study will give firsthand view of how culture, via cultural tightness-looseness index, moderates the mobile cyber hygiene behavior of the Chinese. The results of this study would offer policy makers insights into how they should calibrate their policies, especially by considering social factors like cultural tightness and looseness.

4 THEORETICAL DEVELOPMENT

Pioneering studies of information security behaviors has centered around surveys of employees in organizations using ad hoc theoretical or empirical frameworks (Goodhue & Straub, n.d.). In recent years, given the similarity between computer misconducts in organizational settings and criminal behavior in social settings, theories developed in the criminology domain have been adopted as the mainstream foundations for information security research, examples of such “cross-application” includes, but is not limited to, General Deterrence Theory (GDT), Rational Choice Theory (RCT), and Social Control Theory (SCT) (Willison & Backhouse, 2006).

Given this trend and development, there exists scope for an integrated model and theory combining psychology, sociology, and criminology with information security studies. In order to determine how theories from these different spaces could be adapted into an integrated model of cyber security behavior model, this study will review related work of General Deterrence Theory, Theory of Planned Behavior, Protection Motivation Theory and Gelfand Cultural Tightness-Looseness Theory.

5 LITERATURE REVIEW

5.1 CYBER HYGIENE

Cyber hygiene, as the word “hygiene” suggests, is best understood when compared to personal hygiene. Just as human engages in good personal hygiene practices to maintain good health and well-being, engaging in good cyber hygiene practices can keep data safe and well-protected.

Cyber Hygiene is a relatively a new term. It was coined by Vinton Cerf, an internet pioneer, who used the term during his statement to the United States Congress Joint Economic Committee on 23 Feb 2000 (*Statement of Dr. Vinton G. Cerf*, n.d.). It has various meanings and was used loosely in many different context, both in academic and non-academic literature (Maennel et al., 2018). Earlier studies on information system related security behavior have used the term computer security behavior and information system security behavior. As scholars started to expand their studies beyond the organization and technical measures and included individual behavior, the term “hygiene” was incorporated into the models. Stanton et al., (2005) is one of the pioneer scholars to propose “basic hygiene” as one of the categories of user risk behavior. Wang et al., (2007) has proposed the term e-hygiene in which human factor is the major vulnerability of information security.

Most application of the term cyber hygiene describes it as either a set of practices (standards) or a behavior. As common literature describes the term as both a human behavior and technological measure, Cyber Hygiene is subsequently defined as “a set of practices aiming to protect from negative impact to the assets from cyber security related risks.” (Maennel et al., 2018).

Cyber awareness is often associated with cyber hygiene. While hygiene is a set of practices, cyber awareness refers to security knowledge. Good cyber hygiene is usually an outcome of awareness, training, individual's attitudes, peer pressure, motives, and opportunities. In this digital age, with data being the new oil and the most valuable resource, cyber hygiene is essential in ensuring data integrity and the smooth functioning of everything from government to SME. Unfortunately, weak cyber hygiene has resulted in humans increasingly targeted as the weakest link in cyber defense (Accenture Security, 2019) resulting in tremendous financial loss, business disruption, information loss and possibly equipment damage.

There are a few common models explaining Cyber Hygiene or the earlier Information Systems Security Behavior, namely General Deterrence Theory, Theory of Planned Behavior (TPB) (Ajzen, 1991), and Protection Motivation Theory (PMT) (Floyd et al., 2000).

5.2 GENERAL DETERRENCE THEORY

General Deterrence Theory (GDT), originally developed in the criminology domain as a model to explain the behaviors of criminals and anti-social personalities, is most widely relied on for research on IS security behavior. Since the first adaptation of GDT to show how security countermeasures can act as deterrent by increasing perception of the severity and certainty of punishment for misusing information system (Straub, 1990), GDT has been on the forefront of numerous ISSP behavioral research (before the advent of Protection Motivation Theory).

GDT posits that an individual is unlikely to commit criminal acts if the perceived certainty, severity, and celerity of the sanctions against the acts are greater. These sanctions are described as follows:

5.2.1 **Severity of Punishment.**

The more severe a punishment, the more likely that a rational human being will desist from criminal acts. To prevent crime, therefore, criminal law must emphasize penalties to encourage citizens to obey the law. Punishment that is too severe is unjust, and punishment that is not severe enough will not deter criminals from committing crimes.

5.2.2 **Certainty of Punishment.**

Ensuring that punishments take place whenever a criminal act is committed.

5.2.3 **Celerity of Punishment.**

The application of the punishment must also be swift. The closer the application of punishment is to the commission of the offense, the greater the likelihood that offenders will realize that crime does not pay.

The main limitation of GDT to this study is that it is only useful if the target research setting has a mechanism to sanction the user who breaches the security rule. This mechanism is absent in a personal environment.

5.3 THEORY OF PLANNED BEHAVIOR

Theory of Planned Behavior (TPB) is an extension of the Theory of Reasoned Action (TRA) (Ajzen, 1991). It postulates that individual behavior is influenced by attitude, subjective norms, and perceived behavioral control as follows:

5.3.1 Attitude.

It is defined as the individual's positive or negative feelings toward engaging in a specified behavior.

5.3.2 Subjective norms.

This describes an individual's perception of what people important to them think about a given behavior.

5.3.3 Perceived behavioral control.

The third component of TPB, refers to an individual's perceived ease or difficulty of performing or facilitating a particular behavior.

The central factor of TPB is an individual's intention to perform a given behavior. It is defined as intentions that capture all the motivational factors influencing a behavior. TPB differs from TRA as it has an additional predictor of intentions, perceived behavioral control, which refers to a person's perception of the ease or difficulty of performing the behavior of interest.

5.4 PROTECTION MOTIVATION THEORY

Protection Motivation Theory (PMT) model behavioral intentions to change health behaviors (Floyd et al., 2000; Rogers, 1975). It was developed to help explain how to influence risky behavior and to understand how the

components of persuasive message are critical. PMT evolved from fear appeals theory; it posits that an individual's behavior in the face of risk is dictated by their **threat appraisals** and their **coping appraisal**.

Threat appraisal, describes an individual's assessment of the level of danger posed by a threatening event, comprises the following constituents:

5.4.1 **Perceived Vulnerability.**

This is an individual's assessment of the probability of the threatening event taking place.

5.4.2 **Perceived Severity.**

This is the severity of the consequences of the threatening event when it takes place.

Coping appraisal refers to an individual's assessment of his or her ability to cope well and avert the potential loss or damage arising from the threat. Coping appraisal is made up of the following constituents:

5.4.3 **Self-Efficacy.**

This is the individual's ability of judging his or her capabilities to cope with or perform the recommended behavior. In the context of information security behavior, it refers to the skills and measures needed to protect the organization's information.

5.4.4 **Response Efficacy.**

This relates to the belief about the perceived benefits of the action taken by the individuals. In the context of information security behavior, it refers to compliance of ISSP as an effective means for detecting a cyber threat.

5.4.5 **Response Cost.**

This is the perceived opportunity costs in terms of monetary, time, effort expended in adopting the recommended behavior.

PMT was created to determine the predictors which raise fear in a person, resulting in a cognitive process to adopt a behavior that will protect him/her from the outcome of the fear (Rogers, 1975). So far, PMT has been applied successfully to health-related issues, injury prevention, political issues, protection issues, environmental concerns, online privacy, and home wireless security (Floyd et al., 2000; Woon et al., 2005; Youn, 2005). This suggests that the theory could be generalized to a wide range of threats that an individual can effectively respond to by performing a given response. Since information security is increasingly about getting people to respond to threats with a given action (Panko, 2004), and computer security is also often known as computer health (Kearns, 2006; Lacy et al., 2006), Protection Motivation Theory is expected to offer insight when applied to the information security setting. Currently, there are numerous studies which adopt PMT to provide theoretical explanation as to why people perform certain countermeasures to detect and prevent computer threat (Crossler, 2010; Crossler & Belanger, 2014; Verkijika, 2018; Hanus & Wu, 2016; Crossler & Belanger, 2014; Heath & Rao, 2009).

5.5 CULTURAL TIGHTNESS-LOOSENESS

Understanding cultural differences and its impact has always been the holy grail of psychology. Cross cultural research is critical to assist organizations manage cultural differences as they continue to expand globally. One of the earliest research to explain cultural differences has been Individualism and Collectivism. It has been developed as the leading constructs explaining how cultures differ (Hofstede, 1980). Individualism implies a loosely knit social framework in which people are supposed to take care of themselves and their immediate family only, while collectivism is characterized by a tight social framework in which people distinguish in-groups and out-groups, where they expect their in-group (relatives, clan, organization) to look after them, in exchange, they feel they owe absolute loyalty to their in-group.

Another dominant concept underpinning cross-cultural organizational research is **values**. It is a broad construct that psychologists have studied for decades. However, despite its broad applicability and ease of measurement, numerous empirical studies seem to suggest that values do not always have adequate explanatory power in understanding cultural differences. Theoretically, numerous scholars are concerned that extensive focus on values in cross-cultural research reflects a subjectivist bias, where culture is reduced to factors that exist inside the individual's head (Earley & Mosakowski, 2002). Although values have dominated research in the field of cultural differences, there is a growing recognition for a new perspective to supplement this approach. Hence, the birth of multi-level theory of **cultural tightness-looseness**.

Pelto (1968), an anthropologist, was the first to divide cultures into tight and loose societies based on their social norms. He identified societies such as Japanese, as examples of tight societies, in which norms were expressed very clearly and unambiguously and in which severe sanctions were imposed on those who deviated from norms. He also identified loose cultures, e.g., Thais, in which norms were expressed through a wide variety of alternative channels, and in which there is a general lack of formality, order and discipline, and a high tolerance for deviant behavior. He also identified numerous antecedents of tightness-looseness, e.g., population density, kinship system, and economic system. For example, an agricultural society would be tighter than hunting and gathering societies, as an agricultural society would require more rigid norms to facilitate coordination to plant and harvest crops.

Tightness-looseness concept has also been employed by scholars in sociology (Boldt, 1978) and psychology (Berry, 1967). In sociology, Boldt and his colleagues have shown that agricultural societies have clearly defined role expectations that leave little room for improvisation, whereas hunting and fishing societies have ambiguous role expectations that enable individuals to exercise their own preferences. In psychology, Berry has observed that individuals in tightly structured agricultural settings (e.g., the Temne of Sierra Leone) exhibited lower psychological differentiation (i.e., a reduced sense of separation of the self from others), as compared with individuals in loosely structured hunting and fishing settings (e.g., Eskimos). Apart from ecological threats (availability of resource e.g., fishing or hunting for food or farming for food), societal tightness and looseness is also associated with organizational context and threat exposure (e.g., warfare). Within organizational context, high

risk organizations (e.g., in nuclear power plant) are expected to be tighter compared with low-risk organizational system, as extensive rules and monitoring are required to be in place to control the inherent risk of the task. Such tighter control of high risk organization exist regardless of the societal cultural context (Gelfand et al., 2006). In Chua et al. (2019) mapping of cultural tightness across China's 31 provinces, he has observed that provinces which were badly damaged and occupied by the Japanese during World War II, tend to have higher cultural tightness. This observation has also extended to provinces located near national border with another country.

With psychology, sociology and anthropology all showing promises of tightness-looseness for understanding cultural differences, the study of external constraints via cultural tightness and looseness has evolved into a viable alternative for values-based research.

Cultural tightness refers to the extent to which (1) social norms are clear and pervasive in a society; and (2) deviations from these norms are not tolerated and maybe punished (Gelfand et al., 2006)

Cultural looseness, in contrast, refers to societies where norms are less clear and a range of behaviors deviating from norms are tolerated.

The theory of cultural tightness-looseness connects societal constraints, e.g., the strength of social norms and sanctions, with individual's psychological behavior. Hence, it is invaluable to determine its main and moderating effects on the predictors of cyber hygiene behaviors. For example, in a tight society, societal institutions generally enforce rules abidance, and its criminal justice system would usually have a wide range of offenses and greater likelihood of punishment. Under such circumstances, individuals are expected to have a

heightened sense of Felt Accountability, where they feel that their actions are constantly being scrutinized, thus resulting in more self-monitoring and awareness. This in turn would result in a strengthening of predictors that enforce cyber hygiene.

Conversely, in a loose society, with less range of offences and less likelihood of punishment, and where individuals are generally more willing to engage in risk taking activity and innovation, individuals' propensity to adopt cyber hygiene will be weakened.

Difference in traits between Culturally Tight and Culturally Loose societies is summarized in **Table 1 Culturally Tight vs Culturally Loose**

Insert Table 1 about here

6 RESEARCH QUESTION

Building on extant research on information security risk, which revolves around organization and desktop computers, and applying psychological models which have been adapted to explain the process individuals undergo in making decisions about performing security measures, our study attempts to understand the impact of cultural norm into existing studies. The research question framed is as follows:

RQ: Does cultural norms (as defined under Cultural Tightness-Looseness theory) affect the adoption of protective behavior and how does it moderate the effects of predictors (under Protection Motivation Theory) on adoption of such behaviors?

The study attempts to answer the research questions as follows:

- (1) Develop an integrated theory model which applies Gelfand Cultural Tightness and Looseness Theory as both predictor and moderators (of predictors under Protection Motivation Theory) to study information security behavior studies,
- (2) Conduct a mobile cyber hygiene survey in China.
- (3) Test the results of the mobile cyber hygiene against the hypothesis of the integrated theory.
- (4) Explain the conclusions, limitations, and future research for the integrated theory.

7 RESEARCH MODEL

Using Gelfand's Cultural Tightness-Looseness model, and building on the studies of Protection Motivation Theory on information security behavior, our research model to answer the research question is depicted below:

Insert Figure 1 about here

The key focus of the model is to capture the relationship between cultural norms (Cultural Tightness-Looseness theory) and individual protective intentions and behaviors.

In addition to the main effects, I will also investigate the moderating effects of cultural norms by interacting the provincial cultural tightness-looseness score with the 5 main predictors of Protection Motivation Theory. PMT has been extensively researched and proven to be a reliable theory. It has been applied successfully in numerous domains especially health related field, injury prevention and adoption of vaccination, to list a few. Since adopting cyber protective measures on end user device is similar to encouraging people to adopt health related hygienic practices, a good fit is expected when adapting this framework to mobile cyber hygiene. Drawing on existing research of PMT predictors on individual security behaviors for this study also enable the results to be readily compared and if required, subsequently expanded for future research. This approach also enables the use of validated questionnaires and scale, hence minimizing error in the data capturing process.

Most extant research on PMT usually adopts intention only models, which postulates that intention is a good predictor of behaviors. However, depending on whether the protective behavior is single or multi-action, the postulation may not be always accurate. Protective cyber measures, as captured by Mobile Cyber Hygiene, mostly comprise multi-action behaviors. Consequently, it is imperative that explicit Mobile Cyber Hygiene Behavior be captured in the model to establish the relationship between intentions and behaviors.

8 HYPOTHESES

Based on the preceding research model, I develop a list of hypotheses with main effects and hypotheses with moderating effects, using the Theory of Cultural Tightness-Looseness and Protection Motivation Theory.

To better understand the hypotheses, I will illustrate with a hypothetical country known as Dragonland. It is a big country with a long history. Geographically, it has both a long coastline and deep inland. The population is concentrated near coastline cities where trading takes place. The country's capital and main institutions are also situated along the coastline. Law enforcement employees per capita along the coastline is generally much higher than the inland. Most people living in coastline cities are working class, working in big SOE (State Owned Enterprise). In the inland, which is sparsely populated, the people are generally farmers or shepherds. Using the theory of Cultural Tightness-Looseness, people living in coastline cities are culturally tight while people living in the inland are culturally loose.

After a serious cyber breach through a senior public servant's mobile phone compromised troves of confidential email exchange among senior public servants and political office holders, the leaders of Dragonland decided to mobilize the whole of government to encourage its people to install MalShieldX, a malware shield developed by the country's national laboratories.

8.1 MAIN EFFECTS

The theory of cultural tightness-looseness connects societal constraints, e.g., the strength of social norms and sanctions, with individuals' psychological behavior. Apart from its moderating effects on the predictors of cyber hygiene

behaviors, it is also invaluable to determine its main effects on mobile cyber hygiene. At a societal level, a tighter society would enforce narrow socialization in its education system, a more restrictive and regulated media environment, and more sanctions and punishments on a wider range of offences. At a psychological level, individuals in a tight society would have a higher degree of felt accountability, whereby they feel a heightened scrutiny of their actions and expect deviance from norms to be met with punishments. They would also adopt ought self-guides, which is what a person believes is his/her responsibility, rather than ideal self-guides.

On the whole, in a culturally tight environment, it is expected that the restrictive environment, heightened individual awareness and self-regulation, will compel an individual to be prevention focus, i.e., comply to cultural and social norms and avoid mistakes. Given protective measures like mobile cyber hygiene are fear driven and prevention in nature, it is hypothesized that cultural tightness has a positive relationship with mobile cyber hygiene intention.

For example, Dragonland has embarked on a vast marketing campaign to encourage its populace to install MalShieldX on their mobile phones. Its marketing message includes shaming individuals (heightened individual awareness) who have not installed MalShieldX on their mobile phones. It has also mandated MalShieldX on all public and civil servants' mobile phones. All contractors engaging with the public or civil service are also mandated to install MalShieldX. Incentives and disincentives are meted out to organizations who meet or do not meet the adoption rates respectively, as stipulated by the central government.

H1: *Cultural Tightness has a positive effect on Mobile Cyber Hygiene Intentions.*

8.1.1 Threat Appraisal

Threat appraisal is defined as an individual's assessment about the level of danger posed by a security threat. It comprises Perceived Security Vulnerabilities and Perceived Security Severity. *Perceived Security Vulnerabilities* is an individual's assessment of the probability of a threatening security event occurring. Numerous studies have concluded that as a person's perception of risk increases, he will be more averse to participating in risky activities and will be more likely to take steps to protect himself from risk (Jarvenpaa & Staples, 2000; Pavlou, 2003; Youn, 2005). Overlaying this observation to the cyber space, Pavlou (2003) has observed that a person's intention to enter into electronic transaction decreases as perceived risk increases. Youn (2005) has also observed that people practicing coping behavior to protect their personal information (e.g., providing false information or incomplete information) are also less likely to provide information to websites. Thus, it is hypothesized that there is a positive relationship between perceived security vulnerabilities and adoption of mobile cyber hygiene.

H2: *Perceived security vulnerabilities has a positive effect on mobile cyber hygiene intentions.*

Perceived Security Severity is the individual's assessment of the severity of the consequences arising from a threatening security event. Likewise, from the studies undertaken to investigate the individual's security behavior on security event, both the probability of the security event taking place and the severity of the security event will result in the individual taking steps to protect himself from the risk.

H3: *Perceived security severity has a positive effect on mobile cyber hygiene intentions.*

8.1.2 Coping Appraisal

Broadly defined, Coping Appraisal is an individual's assessment of his ability to cope with and avert the potential loss or damage resulting from the threatening security event (Crossler, 2010). Under PMT, coping appraisal is one of the determinants whether a person adopts a given behavioral response (Floyd et al., 2000). Neuwirth et al. (2000) has shown that a person's coping appraisal increased his willingness to perform the coping behavior. It comprises *security self-efficacy* and *response efficacy*.

Security Self Efficacy is an individual's confidence in his/her own ability to perform the recommended behavior to prevent or mitigate the threatening security event. Extant study using instruments known as computer self-efficacy has observed that computer self-efficacy influenced the expectations of the individual on the outcome of using computers (Compeau & Higgins, 1995). Properly contextually adapted, Marakas et al. (2007) found that computer self-efficacy is a good predictor of performance. Verkijika (2018)

concluded that in order for an individual to adopt good security behaviors to protect their smartphones, it is expected that they strongly believe in the skills they possess to protect their devices.

Bandura (1997) has defined five factors that influence self-efficacy: mastery experience, vicarious experiences, verbal persuasion and physiological/affective differences. These factors vary according to the socio-cultural environments. In a quasi-experimental study conducted by Little et al. (1995), they found that Russian and German pupils had significantly lower self-efficacies as compared to American pupils. They theorized that the lower efficacies of Russian and German pupils are a result of three factors as follows:

8.1.2.1 Degree of Dimensionality.

The Russian and German curricula were unidimensional - uniform and similar for all pupils; while the American curricula was multidimensional - there were more cooperative and individualized learning opportunities, addressing individual learning needs. While it is harder for American students to experience “self-mastery” in a multidimensional curriculum, the fact that their teachers constantly setup the pupils for success and constantly praised students’ efforts (a form of verbal persuasion), raised the self-efficacies of American students as compared to Russian and German students, who are subjected to more competitive feedback and less individualized praises (less verbal persuasion).

8.1.2.2 Feedback Directness.

American teachers often praised student partial success and effort, while Russian and German teachers were more critical and usually used corrective

statements. Consequently, the reduced critical orientation of American feedback helps build confidence and raise self-efficacies as compared to the more critical feedback of the Russian and German.

8.1.2.3 Feedback Transparency.

This refers to the degree of public or private feedback which would affect an individual's self-perceptions of mastery experience. America's relatively lower levels of comparative self-reflection, coupled with the teacher's esteem building feedback (private feedback), is likely to elevate self-efficacy levels as compared to Russian and German critical and public feedback (in front of the class).

Hence, it is expected that security self-efficacy will have a positive effect on mobile cyber hygiene intentions.

H4: *Security self-efficacy has a positive effect on mobile cyber hygiene intentions.*

Response efficacy is the confidence a person has that a given response will mitigate or reduce a threat. Venkatesh et al (2003), has shown that increased outcome expectations led to intention to use a technology. Hence it is expected that as response efficacy increases (like outcome expectations), the security behavior of individuals on adopting mobile cyber behavior will increase.

H5: *Response efficacy has a positive effect on mobile cyber hygiene intentions.*

Response cost is the opportunity cost (time, cognitive effort, financial resource) required to mitigate the security threats and it has a negative effect on mobile cyber hygiene. Numerous studies have shown that as the cost of adopting a technology (including cost of time and effort) increases, an individual becomes less likely to use the technology (Wu & Wang, 2005).

Example. While the new MalShieldX software has been designed with the end user in mind, it suffers from huge battery drained. The typical battery life of a mobile phone reduces 30% after installing of the MalShieldX. In addition, there are numerous cases of early adopters of the software encountering phone overheating or freezing issues. As such the adoption of the application has been very slow.

H6: *Response cost has a negative effect on mobile cyber hygiene intentions.*

8.2 MODERATING EFFECTS

Culturally, a tight society has narrow socialization reinforced by their educational institution, media, and criminal justice system. Such pervasive rules, monitoring of behavior and wider range of punishable offences due to narrower socialization results in more self-awareness and self-monitoring. Consequently, threats are accentuated as people are socialized to its consequences. Hence, narrow socialization coupled with accentuated threats heightened risk perception, in this context perceived security vulnerabilities. Conversely, a loose society will downplay perceived security vulnerabilities due to its broader socialization, lower felt accountability and risk seeking behavior.

Thus, it is hypothesized that a tight society will strengthen the positive effects of perceived vulnerabilities on mobile cyber hygiene intentions as follows:

Example. Dragonland has labelled the recent cyber breaches as a “collective threat” to the nation. News of personal cyber vulnerabilities top the newspaper headlines for weeks. This message of vulnerabilities spread rapidly along the coastline cities. All SOE companies are required to report to the central government the progress of MalShieldX adoption within their company, with incentive for rapid adoption and “admonishment” for poor adoption. However, the people living inland are more indifferent to these messages. This is partly due to the fact they lived further away and generally are indifferent to such “headlines”. Most of them are independent farmers and do not work under SOE. Consequently, there are less touchpoints with the government and the incentives and disincentives for adoption are irrelevant to them. The adoption rate of MalShieldX for people along the coastline cities (culturally tight) is much higher than the people staying inland.

H7: *The tighter the culture, the stronger the positive effects of perceived security vulnerabilities on mobile cyber hygiene intentions.*

Similarly, the moderating factors of a culturally tight environment will strengthen the positive effects of the perceived security severity, while a culturally loose environment will weaken the positive effects of the perceived security severity.

Example. Message of mobile phone vulnerabilities and severity hit the headlines of official newspapers regularly. There is even anecdotal evidence of

whole communities of people being investigated due to actual (or even potential) security breach of their mobile. The official tagline is that cyber breaches can destroy families and such anecdotal stories reinforced the message. While companies are being “admonished” for low adoption rate, they are shamed on national TV, should cyber breach take place within their premises. Hence the working class people, living along the coastline cities, adopts the MalShieldX readily. Deeper inland, the loose social norms due to geography and the economic model where most people are either farmers or shepherds, the repercussions of maladaptive behaviors do not resonate as closely.

***H8:** The tighter the culture, the stronger the positive effects of perceived security severity on mobile cyber hygiene intentions.*

There are numerous commonalities when comparing Little’s (1995) study with Cultural Tightness and Looseness theory. The factors elevating American’s self-efficacies can be equated to the broad socialization associated in a loose society. Just like the multidimensionality of America curricula, educational institution of loose society encourages exploration and metes out less punishment. Collectively, loose society adopts a form of verbal persuasion which elevates self-efficacy. Conversely, the critical feedback of Russian and German system is similar to the more restricted and regulated environment of a tight society where deviant behavior is discouraged, criticized or even punished.

Given these similarities, our study hypothesized that tight culture would weaken the positive effects of security self-efficacy, leading to weaker mobile cyber hygiene intentions. Conversely, loose culture will elevate self-efficacy

and strengthen the effects of security self-efficacy, leading to stronger mobile cyber hygiene intention.

Example. Through the years, a strong community network has developed in the coastline cities. While such networks were used to coordinate neighborhood policies, they are now used to coordinate wide acceptance of MalShieldX. It helps conduct official training to lower the barriers of adopting MalShieldX. Individual gripes of the application were also discouraged and privately dealt with. Consequently, the anxiety over the initial shortfalls of MalShieldX raised by early adopters were mitigated. Inland communities do not have such networks and hence gripes raised by early adopters are still prevalent and foreshadowed any installation of MalShieldX.

H9: The tighter the culture, the weaker is the positive effects of security self-efficacy on mobile cyber hygiene intentions.

In a tight society, messages are spread more rapidly and pervasively. Individuals also tend to adopt prevention focus which is prevalent in societies driven by criticism. They consider what might go badly if they do not work hard enough to achieve. Prevention focused people are often conservative and do not take chances. Hence, it is hypothesized that if a given response is shown to reduce or mitigate a threat, its positive effects would be strengthened in a culturally tight society.

Example. The omnipresent community networks of tighter communities along the coastline cities help disseminate the message of the importance and effectiveness of MalShieldX more pervasively and rapidly.

H10: *The tighter the society, the stronger the positive effects of response efficacy on mobile cyber hygiene intentions.*

Adoption of information security measures would often require strict adherence to certain protocols (e.g., ensuring authenticity of email would require additional checks and possibly launch of anti-virus/anti-phishing application) that hinder seamless operation and frustrate speedy operation, the latter is frustrating in a culturally loose environment. In some culturally tight society, the whole organization or even government might be “cut-off” totally from the public internet to prevent unauthorized access to their sensitive information. For example, in 2016, the Singapore government announced that they were cutting internet connection from all computers used by public and civil servants in the public service and ministries respectively (Tham, 2016). While the resource of the world wide web is still available (via separate workstations and only given when one is of high seniority), the cost of “response”, which is the near total cut-off from the internet, is very high as information is no longer at the user’s fingertips. Also, any importation of internet resource would require numerous levels of authentication and approval.

Such strict rule abidance and monitoring, however, is a hallmark of a tight society. They have more well-developed system for monitoring performance and have greater order, precision, cohesion, and higher efficiency. Tight cultures are better designed to manage cost and follow rules. Conversely, loose cultures have less order, and their individuals are undisciplined and less attentive to discrepancies. They are thus not optimally designed to manage rules and control cost.

A study on the impact of culture on price elasticity, however, provides a different explanation. Using Hofstede cultural dimension construct, Kemper (2018) observed that culture with high power distance, individualism and masculinity is less sensitive to price fluctuations. This is due to the need to project social status and position in the society. Consequently, they are willing to pay a price premium to show their ability to purchase the service.

In comparison, in cultural tightness-looseness theory, tight cultures tend to be associated with long term orientation and a collectivist mindset. When combining these observations with cultural tightness-looseness theory, I theorize that fluctuation in response cost tend be felt greater in tight cultures. Thus, the effects of response cost on adoption of cyber hygiene are more pronounced in a tight society.

As extant study on effects of response cost on tight society are conflicting, that it is both better managed and more sensitive to price fluctuations, I will theorize two opposing hypothesis to be validated as part of data survey as follows: (1) the negative effects of response cost on adoption of mobile cyber hygiene intention is weakened in a tight society when compared to a loose society in consideration of its cost management; (2) the long term orientation of tight society results in more sensitivity towards price fluctuations.

Example A. The SOE inside coastline cities are given tax incentives for achieving a high adoption rate of MalShieldX. Hence existing team structures within SOE were tasked to accelerate adoption of MalShieldX. Adoption rate of MalShieldX were also incorporated into weekly meetings agenda and defined as cardinal key success factors (KSF) for close monitoring. Consequently, the

adoption rate of MalShieldX along the coastlines are high due to employment of existing tight management structure.

H11a: The negative effects response cost on mobile cyber hygiene intentions are weaker in a tight culture when compared to a loose culture.

Example B. The numerous SOE inside coastline cities scrutinized the effort to accelerate deployment of MalShieldX and found that the resource for this effort will affect productivity and both near term and mid-term objectives. As a result, numerous SOE decided to prohibit discussion of MalShieldX in their weekly meetings and social gatherings. The purpose is to maintain focus on productivity and achieving central government's objective. Consequently, "chatter" on MalShieldX reduced and its adoption rate dropped dramatically.

H11b: The negative effects of response cost on mobile cyber hygiene intentions are stronger in a tight culture when compared to a loose culture.

8.3 INTENTIONS AND BEHAVIORS

While most information security studies adopt intention-based model (e.g. PMT) which posits that behavioral intentions predicts actual behavior, it is not uncommon to find cases where this postulation does not hold true (Ajzen et al., 2004). Sheeran observed that the relationship between intentions and behaviors are stronger for single-action behavior when compared to multi-action behavior (Sheeran, 2002). Thus, there has been studies that designed to take into consideration the actual security behavior (since information security

behaviors are mostly multi-action behavior) and concluded that there's significant positive relationship between information security intentions and behaviors (Liang & Xue, 2010; Thompson et al., 2017). Extrapolating from this research, my study postulates that mobile cyber hygiene intentions have a positive relationship with mobile cyber hygiene behaviors.

***H12:** Mobile Cyber Hygiene Intentions has a positive relationship with Mobile Cyber Hygiene Behavior.*

8.4 SUMMARY OF HYPOTHESES AND RESEARCH MODEL

Insert Table 2 and Figure 2 about here

9 METHODOLOGY

9.1 SAMPLE AND DATA COLLECTION

In this study, the target population is the mobile phone users in China. A 3rd party sample service provider, online survey company (www.wjx.cn), was engaged to recruit at least 100 participants from each of the 31 provinces cum cities in China. The mobile questionnaire survey will collect data on the independent variables, dependent variables, moderators, and control variables of the research model. As required under the IRB, all respondents are at least 18 years old, and specifically no respondents are pregnant. Respondents would first answer several background questions (control variables) about themselves. In addition, it will utilize the cultural tightness index across 31 provinces in China (Chua et al., 2019) to explore its' moderating effects on the data collected.

9.2 MEASURES

The research model defines the following variables:

9.2.1 Independent Variables (Predictors).

Perceived Security Vulnerabilities (PV), Perceived Security Severity (PS), Security Self Efficacy (SE), Security Response Efficacy (RE), Response Cost (RC)

9.2.2 Dependent Variables (Response variables).

Mobile Cyber Hygiene-Intentions (MCH-I), Mobile Cyber Hygiene-Behaviors (MCH-B).

9.2.3 **Moderators.**

Cultural Tightness-Looseness (CTLSCORE). This is a score determined by Chua et al. (2019). The index is determined by a series of 6 questions with a value from 1 to 5 where 1 is culturally loose while 5 is culturally tight.

To ensure validity and reliability of the items used to measure the model constructs, relevant measures validated by extant behavioral studies were used, wherever possible. When there is an absence of relevant measures, I make adaptations from relevant measures. For example, our measures of Independent Variables were largely adapted from Thompson et al. (2017) studies. Instead of home computers, I replace the devices with Smartphone.

The constructs measured as modeled were as follows:

9.2.4 **Measures of Protection Motivation.**

The main predictors (perceived security severity, perceived security vulnerability, response efficacy, response cost, and self-efficacy) and responses (mobile cyber hygiene intentions) for the model are adapted from Thomson (Thompson et al., 2017). It comprises a series of 30 questions where each construct of interest was measured on a 7-point Likert Scale from 1 “Strongly Disagree” to 7 “Strongly Agree”.

(1) **Perceived Security Severity (PS).**

A total of 5 questions determining the respondents’ awareness of the severity of cyber-attacks on his/her mobile.

(2) **Perceived Security Vulnerability (PV).**

A total of 6 questions determining the respondents’ assessment of their vulnerability to cyber-attacks.

(3) **Response Cost (RC).**

A total of 6 questions determining the respondents' assessment of cost in terms of time, finance, and effort in order to setup the response against the potential cyber threat.

(4) Response Efficacy (RE).

A total of 5 questions to determine the respondents' confidence that the response is effective against the perceived cyber threat.

(5) Security Self-Efficacy (SE).

A total of 5 questions measuring respondents' confidence in his/her own ability to perform the recommended behavior to prevent or mitigate the threatening event.

(6) Mobile Cyber Hygiene-Intentions (MCHI).

A total of 4 questions to measure the respondents' intentions towards adopting protective measure on their mobile phone.

As each construct is measured by multiple questions, the eventual response of each construct is obtained by computing the mean of the various responses.

9.2.5 Measures of Mobile Cyber Hygiene-B (MCH-B).

The relationship between the intentions and behaviors are measured via a Mobile Cyber Hygiene-Behavior (MCH-B) test that is structured with a 1 "Yes" or 0 "No" reply. The questionnaires under MCH-B were designed to mirror a self-reported behavior measurement. Respondents would complete a total of 17 questions and through the response of these 17 questions (each with a definite answer), a score would be attributed to the respondents measuring his/her mobile cyber hygiene behaviors.

9.2.6 Measures of Personality.

I use the Big Five Personality Test (Rammstedt & John, 2007) to determine the persona of the respondents. There is a total of 10 questions in this questionnaire and scoring the Big Five traits are as follows:

- Extraversion: Question 1(R) and 5
- Agreeableness: Question 2 and 7(R)
- Conscientiousness. Question 3(R) and 8
- Neuroticism. Question 4(R) and 9
- Openness to Experience. Question 5(R) and 10.

This information would enable us to control the effects of personality on the moderating effects of the environment.

9.2.7 Measures of Regulatory Focus.

Finally, I use Higgins Regulatory Focus Test (Higgins et al., 2001) to determine the respondents regulatory focus as another means to control the effects of the environment with the results. The responses of the 11 questions would determine the specific type of regulatory focus as follows:

- Promotion = $[Q1(R) + Q3 + Q7 + Q9 (R) + Q10 + Q11(R)] / 6$
- Prevention = $[Q2(R) + Q4(R) + Q5 + Q6(R) + Q8(R)] / 5$

9.3 DATA SCREENING

Apart from ensuring the respondents were of age 18 and above and that there were no respondents who were pregnant during the survey, 2 additional questions were deliberately inserted at the middle and end of the survey to

ensure the respondents were of sound mind and were not robots. The sample service provider WJX would also remove invalid and suspicious responses.

10 RESULTS

A total of valid 4159 responses (44.1% Male and 55.9% Female) were used in the analysis. Background information of the respondents are detailed below:

Insert Table 3 about here

10.1 RELIABILITY

Cronbach's alpha is a measure used to assess the reliability, or internal consistency, of a set of scale or test items. I use this measure to determine the reliability of the test items.

Insert Table 4 about here

The survey scale has a reasonably strong α coefficient of more than 0.7 based on the data collection. Hence, the items exhibit strong face validity and construct validity.

10.2 APPROACH

I use STATA to analyze the data using general linear model (correlations and linear regression). The relationship of the variables is investigated by gradual layering of control variables, independent variables and moderators into the model as follows:

- (1) Relationship between dependent variables and control variables (e.g., age, education).

- (2) Relationship between dependent variables, controls variables, and independent variables (perceived security severity, perceived security vulnerability, response efficacy, response cost, self-efficacy).
- (3) Relationship between dependent variables, control variables, independent variables, and moderators (moderation between cultural tightness with perceived severity security, perceived security vulnerability, response efficacy, response cost, and self-efficacy).
- (4) Finally, a moderated mediation model was then analyzed using path analysis. The 2 results were then compared for consistency.

10.3 CORRELATION

Insert Table 5 about here

The above table shows the correlation of key variables of the research model. There appears to be positive correlation amongst the independent variables on the response variables. As hypothesized by the model, all the predictors, less Response Cost, have a positive relationship with mobile cyber hygiene intentions.

Likewise, the moderators (represented by the interaction of the predictors with moderators) strengthens the positive effects of the predictors,

less the moderation with Response Cost. This is also what is theorized in the research model.

Lastly, the intentions and behaviors will be positively correlated.

10.4 FIXED OR RANDOM EFFECTS

To determine whether to use fixed or random effects on the panel data, a Hausman test was done and the result $\text{Prob} > \chi^2 = 0.65$. Since the probability is bigger than 0.05, random effects is recommended.

10.5 CONTROL VARIABLES (DEMOGRAPHICS)

Multiple regression is conducted with control variables to see if these variables will predict mobile cyber hygiene intentions. The table below shows that demographics variables have a small albeit significant relationship with mobile cyber hygiene intentions.

Insert Table 6 about here

10.6 MAIN EFFECTS WITH INDEPENDENT VARIABLES

The main effects of the independent variables on mobile cyber hygiene intentions are tested using linear regression. Table 7 shows controlling with demographic variables, all the predictors continue to have a significant relationship with mobile cyber hygiene intentions as theorized. The significance

of control variables was reduced dramatically with only Education remaining to have a significant relationship with mobile cyber hygiene intentions.

Insert Table 7 about here

10.7 MAIN EFFECTS WITH INDEPENDENT VARIABLES AND MODERATORS

In the final regression iteration, all the control variables, predictors and variables are included. Table 8 shows 4 out of the 5 predictors having significant relationship with the dependent variables.

Insert Table 8 about here

On the moderation effect of Cultural Tightness and the predictors, the interaction between Perceived Security Severity and Cultural Tightness-Looseness, and the interaction between Response Cost and Cultural Tightness-Looseness, have shown to be significant. The regression shows a significant positive relationship between Cultural Tightness-Looseness with Mobile Cyber Hygiene Intentions.

A margin plot of the 2 significant interaction effects of cultural tightness-looseness on predictors also confirm the relationship depicted on the table.

Insert Figure 3 and Figure 4 about here

10.8 EFFECTS OF INTENTIONS ON BEHAVIOR

With control variables and cultural tightness-looseness, a regression of mobile cyber hygiene intentions on mobile cyber hygiene behaviors shows a positive relationship between the 2 variables.

Insert Table 9 about here

10.9 MAIN EFFECTS AND MODERATIONS ON MOBILE CYBER HYGIENE BEHAVIORS

Although the model calls for mobile cyber hygiene intentions as a mediator for mobile cyber hygiene behaviors, I took the data and conduct a regression with mobile cyber hygiene behaviors as the dependent variables for the various predictors.

The regression shows a reduction in number of main effects but increase in number of moderation effects. Also, the effects of control variables also increased (see Table 10).

Insert Table 10 about here

10.10 FULL MODEL ANALYSIS USING PATH ANALYSIS (MODERATED MEDIATION)

Finally, path analysis was used to test the model in full. This allows a comparison of path analysis results with regression.

Insert Table 11 and Table 12 about here

11 HYPOTHESES TESTING

11.1 HYPOTHESIS 1 – CULTURAL TIGHTNESS-LOOSENESS HAS A POSITIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression result shows cultural tightness-looseness of the respondent's province positively predicted his or her intentions to adopt mobile cyber hygiene behaviors ($b = 0.279, p=0.039^*$). Turning to correlation results, it shows behavior (mobile cyber hygiene behaviors) is more strongly associated with cultural tightness-looseness than intentions ($b = 0.02$ vs $b = 0.08^*$). In the full model supplementary analysis, cultural tightness score shows a more significant positive effect close to the regression results ($b = 0.284, p=006^{**}$).

The hypothesis is supported.

11.2 HYPOTHESIS 2 – PERCEIVED SECURITY VULNERABILITY HAS A POSITIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression shows a marginally significant results ($b = 0.075, p = 0.111$). The correlation results the association to be significant ($b = 0.212, p = 0.000^{***}$). The results in the full model analysis also show significant relationship ($b = 0.072, p = 0.039^*$).

The hypothesis is not supported by the main regression analysis but supported by correlation and path analysis.

11.3 HYPOTHESIS 3 – PERCEIVED SECURITY SEVERITY HAS A POSITIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression shows a significant positive relationship ($b = 0.23$, $p = 0.000***$). Correlations results is also significant ($b = 0.266$, $p = 0.000***$). Lastly, path analysis shows a similar relationship as regression ($b = 0.233$, $p = 0.000***$).

The hypothesis is supported.

11.4 HYPOTHESIS 4 – SECURITY SELF-EFFICACY HAS A POSITIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression shows a significant positive relationship ($b = 0.311$, $p = 0.000***$). This is supported by the correlation results ($b = 0.54$, $p = 0.000***$) and path analysis result ($b = 0.312$, $p = 0.000***$).

The hypothesis is supported.

11.5 HYPOTHESIS 5 – RESPONSE EFFICACY HAS A POSITIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression shows a significant relationship ($b = 0.338$, $p = 0.000***$). Both correlation ($b = 0.54$, $p = 0.000***$) and path analysis also show significant positive relationship ($b = 0.337$, $p = 0.000***$).

The hypothesis is supported.

11.6 HYPOTHESIS 6 – RESPONSE COST HAS A NEGATIVE EFFECT ON MOBILE CYBER HYGIENE INTENTIONS

The regression result shows a significant albeit small negative relationship ($b = -0.082$, $p = 0.009**$). Correlation shows the

association to be significant ($b = -0.151, p = 0.000***$) while path analysis also supported the relationship ($b = -0.08, p = 0.018^*$).

The hypothesis is supported.

11.7 HYPOTHESIS 7 – THE TIGHTER THE CULTURE, THE STRONGER IS THE POSITIVE EFFECT OF PERCEIVED SECURITY VULNERABILITIES ON MOBILE CYBER HYGIENE INTENTIONS.

Regression of the moderation effects dose not show any significant effect ($b = 0.001, p = 0.610$). Correlation results however shows significant association ($b = 0.129, p = 0.000***$). Path analyses confirm regression results ($b = 0.007, p = 0.506$) with no significant relationship.

The hypothesis is not supported.

11.8 HYPOTHESIS 8 – THE TIGHTER THE CULTURE, THE STRONGER IS THE POSITIVE EFFECT OF PERCEIVED SECURITY SEVERITY ON MOBILE CYBER HYGIENE INTENTIONS

The regression of this moderation shows significant relationship ($b = -0.047, p = 0.000***$). However, the effect is negative instead of the positive as hypothesized. Correlation results a positive relationship ($b = 0.112, p = 0.000***$) while path analysis corroborated regression analysis ($b = -0.049, p = 0.000***$).

The hypothesis is significant but not supported (as the direction of the relationship is different).

11.9 HYPOTHESIS 9 – THE TIGHTER THE CULTURE, THE WEAKER IS THE POSITIVE EFFECT OF SECURITY SELF-EFFICACY ON MOBILE CYBER HYGIENE INTENTIONS

The regression result does not show any significant relationship ($b = 0.014$, $p = 0.535$). The correlation result, however, show positive association ($b = 0.26$, $p = 0.000***$). Path analysis shows similar results as regression ($b = 0.014$, $p = 0.283$).

The hypothesis is not supported.

11.10 HYPOTHESIS 10 – THE TIGHTER THE CULTURE, THE STRONGER IS THE POSITIVE EFFECT OF THE RESPONSE EFFICACY ON MOBILE CYBER HYGIENE INTENTIONS

The regression result is not significant ($b = -0.006$, $p = 0.754$). However, the correlation result shows positive association ($b = 0.23$, $p = 0.000***$), which again is not supported by path analysis ($b = -0.005$, $p = 0.721$).

The hypothesis is not supported.

11.11 HYPOTHESIS 11A/11B – THE NEGATIVE EFFECTS OF RESPONSE COST ON MOBILE CYBER HYGIENE INTENTIONS ARE WEAKER/STRONGER IN A TIGHT CULTURE WHEN COMPARED TO A LOOS CULTURE

The regression result supports the weakening of the negative effect ($b = -0.016$, $p = 0.058*$). This is supported by correlation ($b = -0.09$, $p = 0.000***$) and nearly so by path analysis ($b = -0.017$, $p = 0.109$).

Hypothesis 11a is supported.

**11.12 HYPOTHESIS 12 – MOBILE CYBER HYGIENE INTENTIONS
HAS POSITIVE EFFECT ON MOBILE CYBER HYGIENE
BEHAVIORS**

Regression with the dependent variable replaced by Mobile Cyber Hygiene Behaviors shows a significant positive relationship ($b = 0.039$, $p = 0.000^{***}$). Correlation also shows similar relationship ($b = 0.323$, $p = 0.000^{***}$). Lastly, the path analysis also shows supports the relationship ($b = 0.013$, $p = 0.000^{***}$).

The hypothesis is supported.

12 SUPPLEMENTARY ANALYSES

Additional data, Regulatory Focus and Big Five Personality, were captured by the survey. Regulatory Focus Theory is a goal pursuit theory which examines the relationship between the motivation of a person and the way in which they go about achieving their goal. The theory is based on the Hedonic principle that people embrace pleasure but avoid pain. In the theory, there are 2 approaches how a person goes about pursuing their goal: (1) Promotion Focus, where the focus is concerned about attaining advancement and accomplishment; and (2) Prevention Focus, where the focus is on security and safety by following guidelines and rules. The survey captured the respondents regulatory focus using Higgins Regulatory Focus Questionnaire.

By controlling for Regulatory Focus (constructs Prevention Focus and Promotion Focus) into the list of predictors for the model, the main effects relationship between Perceived Security Vulnerability and Mobile Cyber Hygiene Intentions become significant ($b = 0.08$, $p = 0.079$). Prevention Focus also has a direct positive relationship with Mobile Cyber Hygiene Intentions ($b = 0.04$, $p = 0.017^*$). This outcome is consistent with Cultural Tightness-Looseness Theory, whereby a tighter society is associated with more Prevention Focus goal pursuit and decision making. As such, it would have a positive relationship with adoption of Mobile Cyber Hygiene Intentions. Perceived Security Vulnerability, which previously has not shown to have significant positive relationship with Mobile Cyber Hygiene Intentions, is now shown to have significant positive effect when including Regulatory Focus predictors. The effects of moderations before regressing with controls and after controlling for Regulatory Focus remains the same.

Insert Table 16 about here

Big Five Personality is psychological trait theory which uses 5 broad dimensions to describe human personality: (1) Extraversion (outgoing/energetic vs solitary/reserved); (2) Agreeableness (friendly/compassionate vs critical/rational); (3) Openness to Experience (inventive/curious vs consistent/cautious); (4) Conscientiousness (efficient/organized vs extravagant/careless); and (5) Neuroticism (sensitive /nervous vs resilient/confident).

Overlaying these personality traits with Cultural Tightness-Looseness Theory, I can associate cultural tightness with these personality traits as follows:

- (1) The tighter the culture, more reserved a person will be. This is because in a more restrictive and regulated environment where deviances from norms are sanctions, a person is likely to be prevention focus (previously explained) and consequently more reserved (and lower Extraversion score).
- (2) The tighter the culture, the less agreeable a person will be. Subject to more research, I theorize that a tighter environment will make a person less agreeable due to their reserve outlook and prevention focus approach.
- (3) The tighter the culture, the less openness to experience a person will be. The more restrictive environment, prevention focus outlook will result in a more cautious personality outlook.

(4) The tighter the culture, the more conscientiousness a person.

Tighter cultures are associated with better management and performance. They are generally more efficient (but less innovative).

(5) The tighter the culture, the more neurotic a person will be. The preventive focus outlook and cautious nature will cause a person to be more nervous and sensitive to triggers.

Controlling for the Big Five personality traits, the predictor Perceived Security Vulnerability is shown to be positively significant. On the moderation effects, only Perceived Security Severity continued to have significant relationship, but the direction is still contrary to hypothesis. The moderation effect on Response Cost became insignificant.

Conscientiousness and Neuroticism is predicted to have positive relationship with adoption of Mobile Cyber Hygiene Intentions. However, the data only shows Conscientiousness having the positive significant relationship. Amongst the negative effect predictors (of Big Five), while Openness to Experience and Extraversion shows negative relationship, the effect is not significant.

Lastly, the data show Agreeableness to be positive associated with Mobile Cyber Hygiene Intentions. This could be explained that as a society become tighter, it is more paramount to ensure collective agreement. Consequently, people are more likely to be agreeable to each other. This could also be a result of more common experience in a tight society.

Insert Table 17 about here

The supplementary analyses show that by controlling for Regulatory Focus the key effects of the regression results remain significant. In fact, the effect of Perceived Security Vulnerability was enhanced. By controlling for Personality, the main effects are similar when controlling for Regulatory Focus. The moderating effects of Response Cost also disappears when controlling for Personality.

Overall, the above analyses show that my results are robust.

13 DISCUSSION

The main regression results supported most of the hypotheses. 4 out of the 5 main effects were significant, while 2 out of the 5 moderations effects were also found to be significant. Cultural Tightness-Looseness is shown to have significant direct effect on mobile cyber hygiene intentions. Mobile cyber hygiene intentions were also shown to have a positive effect on mobile cyber hygiene behaviors. A total of 8 out of the 12 hypotheses were significant while 7 out of 12 were supported.

Insert Figure 5 and Table 13 about here

The model is also found to exhibit goodness of fit, within R square of 0.429 and between R square of 0.539. With an overall R square value of 0.43, the model can explain 43% of the variance in mobile cyber hygiene intentions.

13.1 MAIN EFFECTS

With a coefficient of 0.279 and a p-value of 0.039, the results confirm the novel idea that Cultural Tightness-Looseness has a significant positive direct effect on mobile cyber hygiene intentions and supports the main hypothesis of this study. This is the first direct study of cultural norms and adoption of protective measures on mobile devices.

The remaining main effects of the findings on predictors of Protective Motivation Theory were consistent with previous studies. The positive

relationship between Mobile Cyber Hygiene Intentions and predictor of Mobile Cyber Hygiene Behaviors is also supported and confirmed with a coefficient value of 0.047 and p-value of 0.000, indicating that the integrated model is adequate to predict not only intentions, but also behaviors.

Nevertheless, I offer the following possible explanation on why there is no significant relationship between Perceived Security Vulnerability and Mobile Cyber Hygiene Intentions.

(1) Lack of Cyber Awareness. Cyber-attack predominantly collects personal information. However, China currently still lacks personal information protection law, and the current cyber security law, in place since 2018, define personal information protection as part of national security rather than mechanism to safeguard individual's privacy (e.g., EU GDPR and Singapore PDPA). Hence, it is possible that in the absence of applicable law, awareness of personal cyber-attacks might be inadequate. Consequently, indifference to 3rd party collection of personal information might be a normative behavior in China.

(2) Low Personal Risk Evaluation. More educated individuals are known to be more confident. Consequently, they consciously make "weaker" security decisions as their personal risk evaluation is low. As graduates and post-graduates account for nearly 75% of the response, they could have attenuated the effect of perceived security vulnerabilities on mobile cyber hygiene intentions.

13.2 MODERATOR'S EFFECTS

Although the main hypothesis and PMT predictors were generally well supported, the moderating effects of cultural tightness on the PMT predictors were not all supported. Of the 5 moderating effects, 2 were significant but only 1 supported (Response Cost). It is surprising that out of the 5 moderating effects of cultural norms on PMT predictors, only Response Cost shows significant effect as hypothesized. Contrary to regression, correlation analysis shows significant positive association of cultural tightness on all 5 predictors. However, as this is a novel study, the interaction effects between cultural tightness and protective behavior predictors may not be well understood.

From the regression results, Perceived Security Severity and Response Cost are found to have significant relationship with the Mobile Cyber Hygiene intentions. With a p-value of < 0.001 , the data shows that Cultural Tightness when interacting with Perceived Security Severity, have a weakening effect on the positive relationship between Perceived Security Severity and Mobile Cyber Hygiene Intentions. This contrasts with the hypothesized positive relationship. The difference in direction could be explained as follows:

- (1) Psychological Ownership (PO). Psychological ownership is defined as a mental state in which individuals feel as though the target of ownership is theirs (Pierce et al., 1991). When a person perceives a high level of psychological ownership towards a target, he will view the target as an extension of himself and experience greater perceptions of power and control over the environment associated with the target. Menard et al. (2018) observed that a collectivist society, generally associated with a country with a tight culture, is

less likely to feel that they have responsibility over the target and see the group or society at large as more responsible for the target. Consequently, the respondents felt less responsible for the target and hence weakened the positive effect of perceived security severity on the target.

(2) “Buffer Effect”. Another possible explanation is the perception that in a culturally tight environment, the government is often associated with higher performance and more developed management system with high degree of alignment across different departments/ministries. Given this context, respondents in a culturally tight society might experience “buffer effect”, whereby the severity of any security breaches are assumed to be handled by the state. For example, in island-state Singapore, the citizens have high level of confidence in their government (Ho, 2021). It is not uncommon to see the State taking the initiative to assume responsibility for many societal ills.

Interaction between Cultural Tightness and Response Cost produce a coefficient of -0.016 and p-value of 0.058, the result confirms that moderation of cultural tightness on response cost will reduce the negative effect of response cost on mobile cyber hygiene intentions.

However, 3 of the hypothesized moderation effects were not supported by the regression. The absence of significance with the moderation of Cultural Tightness and Perceived Security Vulnerability could be attributed to the lack of main effects. For Self-Efficacy, absence of significant results could be

attributed to Self-Confidence Theory. Krueger & Dickson (1994) observed that increase in self-efficacy increases perception of opportunity and decreases perception of threat. This contrast with the observation from Protection Motivation Theory. Moderated with Cultural Tightness, the outcome might not be significant.

Lastly with respect to Response Efficacy, the absence of significance could be due to lack of cyber awareness. Hence, the effect is indeterministic upon interacting with cultural tightness.

To determine if the predictors are also applicable for mobile cyber hygiene behaviors, I regressed the data by swapping intentions with behavior as the dependent variable. The result was encouraging. 3 out of the 5 main effects and 3 out of the 5 moderations were significant.

Common among the 2 regression (with different DV), moderation of Perceived Security Severity with cultural tightness was shown to weaken positive effect of perceived security severity on mobile cyber hygiene intentions.

With the available data, I used path analysis to conduct a moderated mediation model analysis and compared the results with regression. On mobile cyber hygiene intentions, path analysis seems to be able to sieve out additional significant relationship perceived security vulnerability. Both regression and path analysis draw similar conclusion on the weakening effect of cultural tightness-looseness moderating on perceived security severity.

Insert Table 14 and Table 15 about here

14 THEORETICAL CONTRIBUTION

This is the first study incorporating cultural norms as a predictor (and moderator) of cyber protective behavior. It contributes to the knowledge of culture by integrating the construct of Cultural Tightness-Looseness with the predictors of Protection Motivation Theory to gain insight on how cultural norms affect end users' intentions on performing protective measures. Specifically, the study examined these moderating effects on the key variables of protection motivation theory. While the latter has been well-researched, cultural tightness-looseness as a modern multi-level theory capable of explaining phenomenon at the psychological and societal level, has yet to be widely used as both predictors and moderators or mediators with other variables.

The findings from this research enrich the repertoire of literature explaining individual security behaviors, specifically towards securing their personal device. Beyond technology, organization structure, leadership and individual traits, culture has demonstrated to have a key impact in the design of security policies in the cyber domain.

15 PRACTICAL IMPLICATIONS

With increasing use of mobile devices for transactions, there's urgency to design policies encouraging end user to adopt protective measures on their devices. This study examines the specific cultural responses to adopting protective measures on end user devices. It enables policy makers to calibrate their policies to achieve better adoption of protective measures. It is the first direct study of the influence of cultural norms on mobile phone users' protective practices.

At the individual level, given the importance of cultural tightness weakening the positive impact of perceived security severity, government bodies and MNCs could embark on training and/or marketing campaign to improve the end user awareness on severity of cyber breaches, especially in culturally tight society, where end user might lower their guard and "delegate" the security of their devices to the government. According to Smith et al. (2002), managers from high power distance culture are also more likely to seek guidance from vertical sources (e.g. their superiors and authorities) rather than lateral sources (e.g. peers). As high-power distance culture is often associated with culturally tight society, messaging for protective cyber hygiene measures should be transmitted via peer social network (e.g., social media like Whatsapp, Facebook etc.) rather than traditional TV media. The messaging should also be relatable and visceral, reinforcing the individual's value as a result of complying with the protective measures and downplaying the role of the government. For example, adopting protective measures would improve job prospects and career growth. Messaging that highlights responsibilities and contribution should be

avoided; the focus should be on the individual's benefits. The authorities could also consider both supraliminal and subliminal stimuli prior to the messaging to make it more effective.

At the national level, this study might compel the government to take more pro-active steps to secure the digital environment. This could manifest in the form of ensuring all end user devices on the market are loaded with "hardened" operating system.

Besides government and individual, this study also illuminates how security culture in an organization could be better enhanced. Instead of generating a new culture, the first step towards a successful security culture is to analyze and examine existing cultural norms among staff. This would help develop sharper and more relatable messaging and robust training for security culture.

Finally, the study explains the conditions which would make social engineering, the most popular form of cyber-attacks, successful. For example, people who are careless with their information are usually from culturally loose societies, and people from cultural tight society tend to downplay risk and even when compromised, refuse to acknowledge in order to avoid punishments.

16 LIMITATIONS

Although this study revealed significant main and moderation effects of cultural tightness-looseness, the absence of more moderation effects on the other variables of protection motivation theory could be further investigated. This could be attributed both to cyber awareness and possibly close similarity of cultural tightness-looseness within the China's 31 provinces. The presence of strong association as shown by correlation there might be underlying variable contributing to the association yet to be discovered and explained by Protection Motivation Theory. A more in-depth theory to uncover latent variables within the interaction of Cultural Tightness-Looseness Theory and Protection Motivation Theory could be conducted. Likewise, an exploratory study between countries with significant cultural tightness-looseness could also be considered to determine if cultural tightness-looseness could have more moderating effects on PMT.

Psychological ownership, a relatively new construct possibly explaining cultural tightness-looseness reverse effect on perceived security severity, could be explored further. It could be either studied as a mediator between predictors and intentions, or as moderator between intentions and behaviors.

Cyber is also a relatively new space, hence there's reason to assume many respondents may not be fully aware of the risk of cyber security and how vulnerable they are to cyber-attacks. Further research could consider conducting the same survey in a controlled setting, where the respondents are first subjected to cyber training such that they are more conscious of cyber breaches severity and their own cyber vulnerability.

Lastly, there is still much scope for improvement to predict respondents' behaviors more accurately from surveys. The original survey involved directing respondents to a website where user behavior can be more accurately determined (via scenario-based simulation on the website) than via survey questions alone. This approach was subsequently abandoned as the sample service provider, in the interest of cyber security (ironically), did not permit survey questions which deviated out of their application platform.

17 CONCLUSIONS

With more and more commercial activities conducted online, the ubiquitous of smart devices, and the rapid acclimatization of work from home (online via desktop/notebooks or mobile), the question of motivating end users to adopt more protective measures would continue. Coupled with diversity in the workplace, deep understanding of cultural impact on securing end user device will be a necessary insight cardinal to a successful security policy, both at national and organizational level.

The findings of this study confirm the importance of considering cultural norms to increase individual's adoption of protective measures on their devices. It proposes cultural norms as a possible explanation as to why certain societies are more prone to social engineering, and consideration of cultural norms to improve success of encouraging more protective behaviors on mobile devices. The cultural tightness-looseness construct should offer new insights to policy makers designing protective cyber policies, and new research streams in the field of protection motivation and individual security behaviors.

18 REFERENCES

- 8 mobile security threats you should take seriously in 2020 | CSO Online. (n.d.). Retrieved December 8, 2020, from <https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html?page=2>
- Accenture Security. (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *Ninth Annual Cost of Cybercrime Study*.
- Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In *Action Control* (pp. 11–39). https://doi.org/10.1007/978-3-642-69746-3_2
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, 30(9), 1108–1121. <https://doi.org/10.1177/0146167204264079>
- Bandura, A. (1997). Self-Efficacy: The Exercise of Control. In *Springer Reference*.
- BERRY, J. W. (1967). Independence and Conformity in Subsistence-Level Societies. *Journal of Personality and Social Psychology*, 7(4 PART 1), 415–418. <https://doi.org/10.1037/h0025231>
- Boldt, E. D. (1978). Structural tightness and cross-cultural research. *Journal of Cross-Cultural Psychology*, 9(2), 151–165. <https://doi.org/10.1177/002202217892003>
- China Internet Network Information Center (CNNIC). (n.d.). The 45th

- Statistical Report on Internet Development in China. China: China Internet Network Information Center (2020). Retrieved December 8, 2020, from <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/hlwtjbg/202004/P020200428596599037028.pdf>
- Chua, R. Y. J., Huang, K. G., & Jin, M. (2019). Mapping cultural tightness and its links to innovation, urbanization, and happiness across 31 provinces in China. *Proceedings of the National Academy of Sciences of the United States of America*. <https://doi.org/10.1073/pnas.1815723116>
- Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly: Management Information Systems*, *19*(2), 189–210. <https://doi.org/10.2307/249688>
- Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. <https://doi.org/10.1109/HICSS.2010.311>
- Dave Kearns. (2006). *Is your Active Directory properly provisioned for network access control?* / *Network World*. Network World. <https://www.networkworld.com/article/2307600/is-your-active-directory-properly-provisioned-for-network-access-control-.html>
- Earley, P. C., & Mosakowski, E. (2002). Linking culture and behavior in organizations: Suggestions for theory development and research methodology. *Research in Multi-Level Issues*, *1*, 297–319. [https://doi.org/10.1016/s1475-9144\(02\)01038-x](https://doi.org/10.1016/s1475-9144(02)01038-x)
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social*

Psychology, 30(2), 407–429. <https://doi.org/10.1111/j.1559-1816.2000.tb02323.x>

Gelfand, M. J., Nishii, L. H., & Raver, J. L. (2006). On the nature and importance of cultural tightness-looseness. *Journal of Applied Psychology*. <https://doi.org/10.1037/0021-9010.91.6.1225>

Goodhue, D. L., & Straub, D. W. (n.d.). *Security concerns of system users A study of perceptions of the adequacy of security* *.

Groysberg, B., Lee, J., Price, J., & Cheng, J. Y. J. (2018). The leader's guide to corporate culture. In *Harvard Business Review* (Vol. 2018, Issue January-February, pp. 44–52).

Higgins, E. T., Friedman, R. S., Harlow, R. E., Idson, L. C., Ayduk, O. N., & Taylor, A. (2001). Achievement orientations from subjective histories of success: Promotion pride versus prevention pride. *European Journal of Social Psychology*. <https://doi.org/10.1002/ejsp.27>

Ho, G. (2021). *Singaporeans have high level of confidence in Government but politically uninterested: IPS study, Politics News & Top Stories - The Straits Times*. Straits Times Singapore. <https://www.straitstimes.com/singapore/politics/singaporeans-have-high-level-of-confidence-in-government-but-politically>

Hofstede, G. (1980). Motivation, leadership, and organization: Do American theories apply abroad? *Organizational Dynamics*, 9(1), 42–63. [https://doi.org/10.1016/0090-2616\(80\)90013-3](https://doi.org/10.1016/0090-2616(80)90013-3)

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: An exploratory study of determinants. *Journal of Strategic Information Systems*, 9(2–3), 129–154.

[https://doi.org/10.1016/s0963-8687\(00\)00042-1](https://doi.org/10.1016/s0963-8687(00)00042-1)

- Kemper, J. (2018). Cross-cultural differences in online price elasticity. In *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*.
- Krueger, N., & Dickson, P. R. (1994). How Believing in Ourselves Increases Risk Taking: Perceived Self-Efficacy and Opportunity Recognition. In *Decision Sciences* (Vol. 25, Issue 3). <https://doi.org/10.1111/j.1540-5915.1994.tb01849.x>
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. <https://doi.org/10.17705/1jais.00232>
- Little, T. D., Oettingen, G., Stetsenko, A., & Baltes, P. B. (1995). Children's Action-Control Beliefs About School Performance: How Do American Children Compare With German and Russian Children? *Journal of Personality and Social Psychology*, *69*(4), 686–700. <https://doi.org/10.1037/0022-3514.69.4.686>
- Maennel, K., Mäses, S., & Maennel, O. (2018). Cyber Hygiene: The Big Picture. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11252 LNCS*, 291–305. https://doi.org/10.1007/978-3-030-03638-6_18
- Marakas, G. M., Johnson, R. D., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*.

<https://doi.org/10.17705/1jais.00112>

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers and Security*.

<https://doi.org/10.1016/j.cose.2011.07.003>

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, 75, 147–166.

<https://doi.org/10.1016/j.cose.2018.01.020>

Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection motivation and risk communication. *Risk Analysis*, 20(5), 721–734.

<https://doi.org/10.1111/0272-4332.205065>

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134.

<https://doi.org/10.1080/10864415.2003.11044275>

Pelto, P. J. (1968). The differences between “tight” and “loose” societies. *Trans-Action*. <https://doi.org/10.1007/BF03180447>

Pierce, J. L., Rubenfeld, S. A., & Morgan, S. (1991). Employee Ownership: a Conceptual Model of Process and Effects. In *Academy of Management Review* (Vol. 16, Issue 1). <https://doi.org/10.5465/amr.1991.4279000>

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. *Journal of Research in Personality*, 41(1), 203–212.

<https://doi.org/10.1016/j.jrp.2006.02.001>

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and

- Attitude Change. *The Journal of Psychology*, 91(1), 93–114.
<https://doi.org/10.1080/00223980.1975.9915803>
- Sheeran, P. (2002). Intention—Behavior Relations: A Conceptual and Empirical Review. *European Review of Social Psychology*, 12(1), 1–36.
<https://doi.org/10.1080/14792772143000003>
- Smith, P. B., Peterson, M. F., Schwartz, S. H., Ahmad, A. H., Akande, D., Andersen, J. A., Ayestaran, S., Bochner, S., Callan, V., Davila, C., Ekelund, B., François, P. H., Graverson, G., Harb, C., Jesuino, J., Kantas, A., Karamushka, L., Koopman, P., Leung, K., ... Yanchuk, V. (2002). Cultural values, sources of guidance, and their relevance to managerial behavior: A 47-nation study. In *Journal of Cross-Cultural Psychology* (Vol. 33, Issue 2). <https://doi.org/10.1177/0022022102033002005>
- Statement of Dr. Vinton G. Cerf.* (n.d.). Retrieved December 2, 2020, from <https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm>
- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255–276. <https://doi.org/10.1287/isre.1.3.255>
- Tham, I. (2016). *Singapore public servants' computers to have no Internet access from May next year.* Straits Times Singapore.
<http://www.straitstimes.com/singapore/singapore-public-servants-computers-to-have-no-internet-access-from-may-next-year>
- Thompson, N., McGill, T. J., & Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. *Computers and Security*, 70, 376–391.
<https://doi.org/10.1016/j.cose.2017.07.003>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User

- acceptance of information technology: Toward a unified view. *MIS Quarterly: Management Information Systems*, 27(3), 425–478.
<https://doi.org/10.2307/30036540>
- Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, 77, 860–870.
<https://doi.org/10.1016/j.cose.2018.03.008>
- Vinet, L., & Zhedanov, A. (2011). A “missing” family of classical orthogonal polynomials. In *Journal of Physics A: Mathematical and Theoretical* (Vol. 44, Issue 8). <https://doi.org/10.1088/1751-8113/44/8/085201>
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*.
<https://doi.org/10.1016/j.cose.2013.04.004>
- Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, 15(4), 403–414.
<https://doi.org/10.1057/palgrave.ejis.3000592>
- Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information and Management*, 42(5), 719–729. <https://doi.org/10.1016/j.im.2004.07.001>
- Youn, S. (2005). Teenagers’ perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. In *Journal of Broadcasting and Electronic Media* (Vol. 49, Issue 1, pp. 86–110).
https://doi.org/10.1207/s15506878jobem4901_6

QUESTIONNAIRE

Variable	Item
Gender Age Living Year Education	Male/Female Years (in bands) Years (in bands) Institutions (in bands)
Part I: Cultural Tightness (Provincial)	6 items for tightness perception
Part II: Measures of Protection Motivation	30 items for protection motivation
Part IIIa: Measures of Mobile Cyber Hygiene Behavior (self-report)	17 items for mobile cyber hygiene behavior
Part IIIb: Measures of Mobile Cyber Hygiene (scenario)	6 items for mobile cyber hygiene behavior
Part IV: Big 5 Personality Test	10 items on respondent's personality
Part V: Regulatory Focus Test	11 items on regulatory focus

Part I: Measures of Cultural Tightness-Looseness

Variables	<p>The following statements refer to [PROVINCE NAME] as a whole.</p> <p>Please indicate whether you agree or disagree with the following statements. Note that the statements sometimes refer to "social norms," which are standards for behavior that are generally unwritten.</p> <p>以下是一些对 XX 省 / 市整体的描述。请根据您的真实情况对以下描述做出评价： 请注意，“社会规范”在 下列说法中是指一些没有被明文规定的社会行为标准</p>	<p>Scale (1-6)</p> <p>Strongly Disagree – 1</p> <p>Moderately Disagree – 2</p> <p>Slightly Disagree – 3</p> <p>Slightly Agree – 4</p> <p>Moderately Agree – 5</p> <p>Strongly Agree - 6</p>
Cultural Tightness	<p>1. There are many social norms that people are supposed to abide in this country.</p> <p>在本省 / 市, 有很多社会规范需要遵守</p> <p>2. In this country, there are very clear expectations for how people should act in most situations.</p> <p>在本省 / 市, 大多数情况下人们很清楚应该如何作为</p> <p>3. People agree upon what behaviors are appropriate versus inappropriate in most situations in this country</p> <p>在本省 / 市, 大多数情况下大家对什么是妥当或者不妥当的行为有很大程度的共识</p> <p>4. People in this country have a great deal of freedom in deciding how they want to behave in most situations (reverse coded)</p> <p>在本省 / 市, 大多数情况下人们可以充分地自由决定作为</p> <p>5. In this country, if someone acts in an inappropriate way, others will strongly disapprove</p> <p>在本省 / 市, 如果有人做出不妥的违规行为会受到来自其他人的强烈的反对</p> <p>6. People in this country almost always comply with social norms</p> <p>在本省 / 市, 人们几乎总是会遵守社会规范</p>	


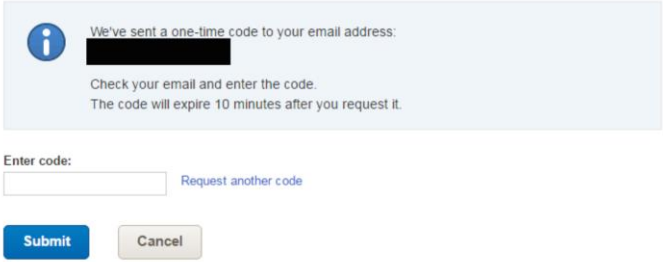
Part II: Measures of Protection Motivation (Self-Report)

	30 Questions	Scale (1-7) Strongly Disagree – 1 Disagree – 2 Somewhat Disagree – 3 Neither Agree/ Disagree – 4 Somewhat Agree – 5 Agree – 6 Strongly Agree – 7
Perceived severity (PS)	<ol style="list-style-type: none"> 1. A security breach on my smartphone would be a serious problem for me 2. Loss of information resulting from hacking would be a serious problem for me 3. Having my confidential information on my smartphone accessed by someone without my consent or knowledge would be a serious problem for me. 4. Having someone successfully attack and damage my smartphone would be very problematic for me 5. view information security attacks on me as harmful 	
Perceived vulnerability (PV)	<ol style="list-style-type: none"> 6. I could be subject to a serious information security threat 7. I am facing more and more information security threats 8. I feel that my smartphone could be vulnerable to a security threat 9. It is likely that my smartphone will be compromised in the future 10. My information and data is vulnerable to security breaches: 11. I could fall victim to a malicious attack 	
Prevention cost (RC)	<ol style="list-style-type: none"> 12. Taking security measures inconveniences me 13. There are too many overheads associated with taking security measures to protect my smartphone 14. Taking security measures would require considerable investment of effort 15. Implementing security measures on my smartphone would be time consuming 16. The cost of implementing recommended security measures exceeds the benefits 17. The impact of security measures on my productivity exceeds the benefits 	
Response efficacy (RE)	<ol style="list-style-type: none"> 18. Enabling security measures on my smartphone will prevent security breaches 19. Implementing security measures on my smartphone is an effective way to prevent hackers 20. Enabling security measures on my smartphone will prevent hackers from stealing my identity 21. The preventative measures available to stop people from getting confidential personal or financial information on my smartphone is effective 22. I believe that protecting the information on my smartphone is important 	

Security Self-efficacy (SE)	<p>23. I feel comfortable taking measures to secure my smartphone</p> <p>24. Taking the necessary security measures is entirely under my control</p> <p>25. I have the resources and the knowledge to take the necessary security measures.</p> <p>26. Taking the necessary security measures is easy to me</p>	
Mobile Cyber Hygiene Intention (MCH-I)	<p>27. I am likely to take security measures on my smartphone</p> <p>28. It is possible that I will take security measures to protect my smartphone</p> <p>29. I am certain that I will take security measures to protect my smartphone</p> <p>30. It is my intention to take measures to protect my smartphone</p>	

Part IIIa: Mobile Cyber Hygiene Behaviors

Security		Yes	No
Behaviors (MCH-B)	<ol style="list-style-type: none"> 1. I install anti-virus/anti-malware products on your mobile phone to protect it from cyber-attack? 2. I backup my mobile phone data periodically. 3. I enabled automatic firmware and apps updates on my mobile. 4. I am aware of threats arising from inadequate security protection on my mobile phone. 5. I am confident I can identify a phishing email or social engineering attack. 6. I am adequately protected from malware, spyware and virus. 7. My passwords are strong and secure. 8. Supposed you're browsing the internet and encounter a website with a green padlock beside the URL. Do you proceed to enter the website? 9. I secure my mobile phone using strong password and/or biometrics. 10. Supposed you receive a phone call where the caller sounds very urgent and require you to do something (e.g., revealing a two-factor authentication code that's just send to your mobile), would you tell him this 2FA code? 11. Supposed you receive a automated voicemail message that informs you that you've an unclaimed parcel and it ask for your private information (e.g., NRIC number and home address) in order to send the parcel to your house, would you give them your private information? 12. Supposed you receive a caller, who identified himself, and give you a number to call back for verifications, would you proceed with calling him/her back? 13. Supposed you are registering an online account with the mobile application, will you use your name or birthday as your password (e.g., ddmmyyyy) 14. Supposed you're browsing the internet and encounter a website with a red triangle beside the URL. Do you proceed to enter the website? 15. You get a text message on your instant messenger or SMS, which says "Congratulations! You've won a cash prize! Click to collect". Would you click the link? 		

	<p>16. Would you reply the following email?</p>  <p>The screenshot shows an email interface with a blue header bar containing 'Reply', 'Forward', and 'Delete' buttons. The email header lists: From: Social Media <support@office365.com>, To: You, Subject: Password Reset Requested. The body features a Windows logo, a paragraph stating a password reset has been requested, a blue 'Reset Password' button with a mouse cursor, and a small callout box with an example URL 'http://office365.com'. At the bottom, it says 'This is an automated email to help protect your account.'</p>	
	<p>17. Would you reply the following email?</p>  <p>The screenshot shows a light blue notification box with an information icon and the text: 'We've sent a one-time code to your email address: [redacted]'. Below the box, it says 'Check your email and enter the code. The code will expire 10 minutes after you request it.' There is an input field for the code, a 'Request another code' link, and 'Submit' and 'Cancel' buttons.</p>	

Part IIIb: Measures of Mobile Cyber Hygiene Behavior (Scenario)

1. Which of the following best describes what is phishing?

- (1) Virus downloaded onto your device.
- (2) Disguised hyperlink and sender address
- (3) Unsolicited requests to fool receivers into divulging personal information.
- (4) Spam mail
- (5) Scam mail (e.g., Nigerian scams)

2. What is anti-virus software used for?

- (1) Disrupt and covertly steal information from your devices.
- (2) Updating your software and systems.
- (3) Protecting your devices against malicious code.
- (4) Securing your password
- (5) Detecting phishing email

3. Which of the following password is the most secure?

- (1) Password
- (2) Boat123
- (3) Pa\$\$wOrd
- (4) 12345
- (5) WTh!56z

4. How do you remember your passwords?

- (1) Reuse the same password for every account.
- (2) Write them down on a piece of paper.
- (3) Keep them in a file on my computer which is password protected
- (4) Share the password with my friends or family members.
- (5) Use a security password manager.

5. You are at a café with free WiFi. Which of the following is the LEAST safe to do?

- (1) Ignore the free WiFi and use your cellular connection.
- (2) Use the free WiFi but secure it with VPN.
- (3) Use the free WiFi but only for general web surfing.
- (4) Use the free WiFi to reply personal email.
- (5) Use the free WiFi to perform personal financial transactions.

6. Which of the following is not recommended over social media?

- (1) Posting photos without editing.
- (2) Sharing locations of your photos
- (3) Sharing photos taken with friends
- (4) Using social media during class or work
- (5) Sharing personal details (e.g. phone numbers, financial information, date of birth) on social media.

Part IV: Big 5 Personality Test

	I see myself as someone who	<p>Scale (1-5)</p> <p>Disagree Strongly – 1</p> <p>Disagree a little – 2</p> <p>Neither Agree/Disagree – 3</p> <p>Agree a little – 4</p> <p>Agree Strongly - 5</p>
Personality Test	<ul style="list-style-type: none"> .. is reserved .. is generally trusting .. tends to be lazy .. is relaxed, handles stress well .. has a few artistic interests .. is outgoing, sociable .. tends to find fault with others .. does a thorough job .. gets nervous easily .. has an active imagination 	

Part V: Regulatory Focus Test

	11 Questions	1 Never or Seldom	2	3 Sometimes	4	5 Very Often
1	Compared to most people, are you typically unable to get what you want out of life?					
2	Growing up, would you ever “cross the line” by doing things that your parents would not tolerate?					
3	How often have you accomplished things that got you “psyched” to work even harder?					
4	Did you get on your parents’ nerves when you were growing up?					
5	How often did you obey rules and regulations that were established by your parents?					

6	Growing up, did you ever act in ways that your parents thought were objectionable?					
7	Do you often do well at different things that you try?					
8	Not being careful enough has gotten me into trouble at times.					
9	When it comes to achieving things that are important to me, I find that I don't perform as well as I ideally would like to do.					
10	I feel like I have made progress toward being successful in my life.					
11	I have found very few hobbies or activities in my life that capture my interest or motivate me to put effort into them.					

Table 1 Culturally Tight vs Culturally Loose

	Culturally Tight	Culturally Loose
Psychological Level	<p><u>Narrow socialization</u> – have more constraint and highly developed systems of monitoring and sanctioning behavior</p> <p><u>Societal Institutions</u> Parents/Teacher – rules abundance, stricter socialization tactics</p> <p>Media – more restricted and regulated in their content.</p> <p><u>Criminal Justice System</u> – wider range of offenses that are punishable; greater likelihood of punishing offenders for crimes offended; stricter sanction for crimes</p> <p><u>Felt Accountability</u> – Subjective experience that one’s action are subject to evaluation and that there are potential punishments based on these evaluations.</p> <p>HIGHER DEGREE of Felt Accountability; feel a heightened scrutiny of their actions and expect violations of norms to be met with stronger punishments.</p>	<p><u>Broad Socialization</u> – lower constraint and weakly developed system of monitoring and sanctioning behavior</p> <p><u>Societal Institutions</u> Parents/Teacher – More exploration, lenient punishment</p> <p>Media – foster broad socialization; open and diverse in their content; subject to fewer regulations, political pressure.</p> <p><u>Criminal Justice System</u> – narrower range of offenses; less likelihood</p> <p>LOWER DEGREE of Felt Accountability</p>
Knowledge Structure	Higher cognitive accessibility of normative requirements	Lower cognitive accessibility of normative requirements
<p><u>Self Guides</u> How external normative context influences psychological processes at individual level</p> <p>Regulatory Focus</p>	<p><u>Ought Self-Guides</u> – What a person believes is his/her responsibility to be?</p> <p>Chronic accessibility of normative ought self-guides</p> <p>Prevention focus (focus on not making mistakes)</p>	<p><u>Ideal Self-Guides</u> – What a person hopes or aspires to be.</p> <p>Chronic accessibility of ideal self-guides</p> <p>Promotion Focus</p>

Decision Making Style	Adaptors – derive ideas using established procedures, cautious, reliable, disciplined.	Innovators – original, risk seeking, undisciplined, impractical, disrespectful of customs → Possible as less felt accountability and less threat of punishments for deviations.
Variance across individuals (personal dispositions, attitudes, expectations)	Share many common experiences (national services in Singapore) -> develop higher between-person similarities.	More varied and idiosyncratic experiences -> individual attributes are more likely to diverge.
<p>Individuals are socialized into the external normative context through key societal institutions.</p> <p>Once socialized, individuals sustain the predominant levels of tightness-looseness by further developing institutions that are consistent with their psychological characteristics</p>		
Innovation	Incremental innovations – R&D funding	Radical Innovations

Table 2 Summary of Hypotheses

Main Effects	
Cultural Tightness-Looseness	
H1	<i>Cultural Tightness-Looseness has a positive effect on mobile cyber hygiene intentions</i>
Threat Appraisals	
H2	<i>Perceived Security Vulnerabilities has a positive effect on mobile cyber hygiene intentions.</i>
H3	<i>Perceived Security Severity has a positive effect on mobile cyber hygiene intentions.</i>
Coping Appraisals	
H4	<i>Security Self-Efficacy has a positive effect on mobile cyber hygiene intentions.</i>
H5	<i>Response efficacy has a positive effect on mobile cyber hygiene intentions.</i>
H6	<i>Response cost has a negative effect on mobile cyber hygiene intentions.</i>
Moderating Effects	
H7	<i>The tighter the culture, the stronger is the positive effect of perceived security vulnerabilities on mobile cyber hygiene intentions.</i>
H8	<i>The tighter the culture, the stronger is the positive effect of perceived security severity on mobile cyber hygiene intentions.</i>
H9	<i>The tighter the culture, the weaker is the positive effect of security self-efficacy on mobile cyber hygiene intentions.</i>
H10	<i>The tighter the culture, the stronger is the positive effect of response efficacy on mobile cyber hygiene intentions.</i>
H11a	<i>The negative effects response cost on mobile cyber hygiene intentions are weaker in a tight culture when compared to a loose culture.</i>
H11b	<i>The negative effects of response cost on mobile cyber hygiene intentions are stronger in a tight culture when compared to a loose culture.</i>
Intentions and Behaviors	
H12	<i>Mobile Cyber Hygiene Intentions has a positive effect on mobile cyber hygiene behaviors</i>

Table 3 Respondent's Demographics

	Male	Female
Gender	44.1%	55.9%
Education		
Primary	< 1%	< 1%
Lower Secondary	< 1%	< 1%
Upper Secondary	2.1%	1.8%
Junior Colleges	1.64%	1.35%
Polytechnics	8.78%	8.49%
University	27.6%	38.95%
Master and above	3.17%	4.4%
Age		
18-25	3.6%	21.6%
26-30	12.21%	13.87%
31-40	13.85%	16.66%
41-50	3.6%	2.93%
51-60	1.47%	< 1%
> 60	< 1%	< 1%

Table 4 Cronbach's Alpha

	Mean	SD	α
Perceived Security Severity (PS)	5.998	0.799	0.8773
Perceived Security Vulnerability (PV)	4.865	1.089	0.8760
Response Cost (RC)	3.833	1.039	0.8821
Response Efficacy (RE)	5.540	0.802	0.8754
Self-Efficacy (SE)	5.236	0.889	0.8762
Mobile Cyber Hygiene Intentions (MCHI)	5.662	0.872	0.8759
Mobile Cyber Hygiene Behaviors (MCHB)	0.738	0.136	0.8662

Table 5 Correlation

S/N	VARIABLE	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Mobile Cyber Hygiene Intentions (MCHI)	1.00												
2	Cultural Tightness-Looseness (CTLSCORE)	0.02	1.00											
3	Perceived Security Severity (PSMEAN)	0.27*	-0.03	1.00										
4	Perceived Security Vulnerability (PVMEAN)	0.21*	0.01	0.37*	1.00									
5	Response Efficacy (REMEAN)	0.54*	0.03	0.33*	0.21*	1.00								
6	Response Cost (RCMEAN)	-0.15*	-0.02	-0.01	0.34*	-0.10*	1.00							
7	Self-Efficacy (SEMEAN)	0.54*	0.04*	0.14*	0.15*	0.48*	-0.00	1.00						
8	PS moderates with Cultural Tightness PSMEAN_CTL	0.11*	0.92*	0.35*	0.15*	0.14*	-0.02	0.08*	1.00					
9	PV moderates with Cultural Tightness PVMEAN_CTL	0.13*	0.82*	0.19*	0.55*	0.13*	0.16*	0.11*	0.84*	1.00				
10	RE moderates with Cultural Tightness REMEAN_CTL	0.23*	0.91*	0.10*	0.08*	0.41*	-0.06*	0.0	0.89*	0.79*	1.00			
11	RC moderates with Cultural Tightness RCMEAN_CTL	-0.09*	0.75*	-0.03*	0.21*	-0.06*	0.61*	0.23*	0.69*	0.74*	0.65*	1.00		
12	SE moderates with Cultural Tightness SEMEAN_CTL	0.26*	0.88*	0.03*	0.07*	-0.24*	-0.03*	0.48*	0.83*	0.76*	0.90*	0.65*	1.00	
13	Mobile Cyber Hygiene Behavior (MCH_BEHAVIOR)	0.32*	0.08*	0.12*	0.02	0.29*	-0.21*	0.37*	0.11*	0.07*	0.19*	-0.08*	0.24*	1.00

Table 6 Regression with Control Variables

	Min	Max	coeff	p-value
Gender (1= Male; 2 = Female)	1	2	-0.054	0.035*
Age	1	6	0.043	0.003***
1 = 18 to 25				
2 = 26 to 30				
3 = 31 to 40				
4 = 41 to 50				
5 = 51 to 60				
6 = > 60				
Education	1	7	0.053	0.001***
1 = Primary				
2 = Lower Sec				
3 = Upp Sec				
4 = Junior College				
5 = Polytechnic				
6 = University				
7 = Master and above				
Provincial GDP (\$billions)	28	1606	-6.35e-06	0.920
Cultural Tightness-Looseness	0.85	5	0.0165	0.439

Table 7 Regression with Predictors

	coeff	p-value
Perceived Security Severity (PSMEAN)	0.080	0.000***
Perceived Security Vulnerability (PVMEAN)	0.094	0.000***
Response Efficacy (REMEAN)	0.323	0.000***
Response Cost (RCMEAN)	- 0.132	0.000***
Self-Efficacy (SEMEAN)	0.357	0.000***
Age	0.006	0.554
Gender	0.002	0.925
Education	0.035	0.000***
Provincial GDP	0.000	0.444
Cultural Tightness-Looseness	0.009	0.552

Table 8 Regression with Predictors and Moderators

	coeff	p-value
Perceived Security Severity (PSMEAN)	0.229	0.000***
Perceived Security Vulnerability (PVMEAN)	0.075	0.111
Response Efficacy (REMEAN)	0.339	0.000***
Response Cost (RCMEAN)	- 0.082	0.009**
Self-Efficacy (SEMEAN)	0.311	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.047	0.000**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.007	0.610
Cultural Tightness-Looseness MODERATED with REMEAN	0.006	0.754
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.016	0.058*
Cultural Tightness-Looseness MODERATED with SEMEAN	0.014	0.754
Age	0.006	0.615
Gender	0.003	0.883
Education	0.035	0.000**
Provincial GDP	-0.000	0.510
Cultural Tightness Looseness	0.279	0.039*

Table 9 Regression of Mobile Cyber Hygiene Intentions on Mobile Cyber Hygiene Behaviors

	coeff	p-value
Mobile Cyber Hygiene Intentions	0.047	0.000***
Age	0.006	0.554
Gender	0.002	0.925
Education	0.035	0.000***
Provincial GDP	0.000	0.444
Cultural Tightness-Looseness	0.009	0.000***

Table 10 Regression with Mobile Cyber Hygiene Behaviors as Dependent Variable

	coeff	p-value
Perceived Security Severity (PSMEAN)	.039	0.000***
Perceived Security Vulnerability (PVMEAN)	-0.000	0.962
Response Efficacy (REMEAN)	0.004	0.658
Response Cost (RCMEAN)	- 0.025	0.000***
Self-Efficacy (SEMEAN)	0.023	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.006	0.004**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.001	0.713
Cultural Tightness-Looseness MODERATED with REMEAN	0.006	0.014*
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.01	0.484
Cultural Tightness-Looseness MODERATED with SEMEAN	0.004	0.036*
Age	0.004	0.073*
Gender	-0.017	0.000***
Education	0.013	0.000***
Provincial GDP	8.11e-06	0.350
Cultural Tightness Looseness	-0.001	0.935

Table 11 Path Analysis (Intention)

	Intentions	
	coeff	p-value
Perceived Security Severity (PSMEAN)	0.233	0.000***
Perceived Security Vulnerability (PVMEAN)	0.072	0.039*
Response Efficacy (REMEAN)	0.337	0.000***
Response Cost (RCMEAN)	-0.081	0.018***
Self-Efficacy (SEMEAN)	0.312	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.049	0.000**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.007	0.506
Cultural Tightness-Looseness MODERATED with REMEAN	-0.006	0.721
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.017	0.109
Cultural Tightness-Looseness MODERATED with SEMEAN	0.014	0.283*
Cultural Tightness-Looseness	0.284	0.006**

Table 12 Path Analysis (Behaviors)

	Behaviors	
	coeff	p-value
Perceived Security Severity (PSMEAN)	0.037	0.000***
Perceived Security Vulnerability (PVMEAN)	-0.002	0.803
Response Efficacy (REMEAN)	-0.001	0.924***
Response Cost (RCMEAN)	-0.024	0.000***
Self-Efficacy (SEMEAN)	0.018	0.017**
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.006	0.011**
Cultural Tightness-Looseness MODERATED with PVMEAN	-0.001	0.759
Cultural Tightness-Looseness MODERATED with REMEAN	0.006	0.027*
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.001	0.618
Cultural Tightness-Looseness MODERATED with SEMEAN	0.004	0.087*
Cultural Tightness-Looseness	-0.004	0.0827

Table 13 Results of Hypotheses Testing

Hypothesis	coeff	p-value	Supported?
H1: Cultural Tightness-Looseness has a positive effect on mobile cyber hygiene intentions.	0.279	0.039*	Supported
H2: Perceived Security Vulnerabilities has a positive effect on mobile cyber hygiene intentions	0.075	0.111	Not supported
H3: The Perceived Security Severity has a positive effect on mobile cyber hygiene intentions.	0.229	0.000***	Supported
H4: Security self-efficacy has a positive effect on mobile cyber hygiene intentions.	0.311	0.000***	Supported
H5: Response efficacy has a positive effect on mobile cyber hygiene intentions.	0.339	0.000***	Supported
H6: Response cost has a negative effect on mobile cyber hygiene intentions.	-0.082	0.009**	Supported
H7: The tighter the culture, the stronger is the positive effect of perceived security vulnerabilities on mobile cyber hygiene intentions	0.007	0.610	Not supported
H8: The tighter the culture, the stronger the positive effect of perceived security severity on mobile cyber hygiene intentions.	-0.047	0.000***	Supported (negative direction)
H9: The tighter the culture, the weaker is the positive effects of security self-efficacy on mobile cyber hygiene intentions.	0.014	0.754	Not supported
H10: The tighter the culture, the stronger the positive effects of response efficacy on mobile cyber hygiene intentions.	0.006	0.754	Not supported
H11a: The tighter the culture, the weaker is the negative effect of	-0.016	0.058*	Supported

response cost on mobile cyber hygiene intentions.			
H11b: The tighter the culture, the stronger is the negative effect of response cost on mobile cyber hygiene intentions	--	--	--
H12: Mobile Cyber Hygiene Intentions has a positive effect on mobile cyber hygiene behaviors.	0.047	0.000***	Supported

Table 14 Comparison of Regression vs Path Analysis (Intentions)

	Intentions (Regression)		Intentions (Path Analysis)	
	coeff	p-value	coeff	p-value
Perceived Security Severity (PSMEAN)	0.229	0.000***	0.171	0.000***
Perceived Security Vulnerability (PVMEAN)	0.075	0.111	0.078	0.026*
Response Efficacy (REMEAN)	0.039	0.000***	0.298	0.000***
Response Cost (RCMEAN)	-0.082	0.009**	-0.114	0.000***
Self-Efficacy (SEMEAN)	0.311	0.000***	0.282	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.047	0.000***	-0.029	0.013**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.007	0.610	0.005	0.612
Cultural Tightness-Looseness MODERATED with REMEAN	0.006	0.754	0.008	0.568
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.016	0.058*	-0.005	0.578
Cultural Tightness-Looseness MODERATED with SEMEAN	0.014	0.754	0.024	0.062*

Table 15 Comparison of Regression vs Path Analysis (Behaviors)

	Behaviors (Regression)		Behaviors (Path Analysis)	
	coeff	p-value	coeff	p-value
Perceived Security Severity (PSMEAN)	0.039	0.000***	0.038	0.000***
Perceived Security Vulnerability (PVMEAN)	-0.000	0.962	- 0.002	0.794
Response Efficacy (REMEAN)	0.004	0.658	- 0.000	0.975***
Response Cost (RCMEAN)	-0.025	0.000***	- 0.024	0.000***
Self-Efficacy (SEMEAN)	0.023	0.000***	0.018	0.011**
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.006	0.004***	- 0.006	0.002*
Cultural Tightness-Looseness MODERATED with PVMEAN	0.001	0.713	- 0.001	0.768
Cultural Tightness-Looseness MODERATED with REMEAN	0.006	0.014*	0.006	0.024*
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.01	0.484	- 0.001	0.525
Cultural Tightness-Looseness MODERATED with SEMEAN	0.004	0.036*	0.004	0.086*

Table 16 Supplementary Analysis with Regulatory Focus Predictors

	coeff	p-value
Perceived Security Severity (PSMEAN)	0.224	0.000***
Perceived Security Vulnerability (PVMEAN)	0.08	0.079*
Response Efficacy (REMEAN)	0.335	0.000***
Response Cost (RCMEAN)	- 0.080	0.012*
Self-Efficacy (SEMEAN)	0.312	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.047	0.000**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.006	0.648
Cultural Tightness-Looseness MODERATED with REMEAN	-0.006	0.767
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.015	0.081*
Cultural Tightness-Looseness MODERATED with SEMEAN	0.014	0.544
Age	0.002	0.814
Gender	0.003	0.899
Education	0.032	0.002**
Provincial GDP	-0.000	0.562
Cultural Tightness Looseness	0.272	0.047*
Prevention	0.04	0.017*
Promotion	-0.000	0.999

Table 17 Supplementary Analysis with Big 5 Personality Traits

	coeff	p-value
Perceived Security Severity (PSMEAN)	0.215	0.000***
Perceived Security Vulnerability (PVMEAN)	0.088	0.064*
Response Efficacy (REMEAN)	0.342	0.000***
Response Cost (RCMEAN)	- 0.077	0.020*
Self-Efficacy (SEMEAN)	0.298	0.000***
Cultural Tightness-Looseness MODERATED with PSMEAN	-0.044	0.000**
Cultural Tightness-Looseness MODERATED with PVMEAN	0.003	0.789
Cultural Tightness-Looseness MODERATED with REMEAN	0.011	0.566
Cultural Tightness-Looseness MODERATED with RCMEAN	-0.014	0.117
Cultural Tightness-Looseness MODERATED with SEMEAN	0.017	0.477
Age	-0.007	0.534
Gender	0.003	0.895
Education	0.030	0.003**
Provincial GDP	-0.000	0.390
Cultural Tightness Looseness	0.279	0.039*
Extraversion	-0.002	0.883
Agreeableness	0.038	0.024*
Openness to Experience	-0.005	0.799
Conscientiousness	0.066	0.000***
Neuroticism	0.008	0.530

Figure 1 Research Model

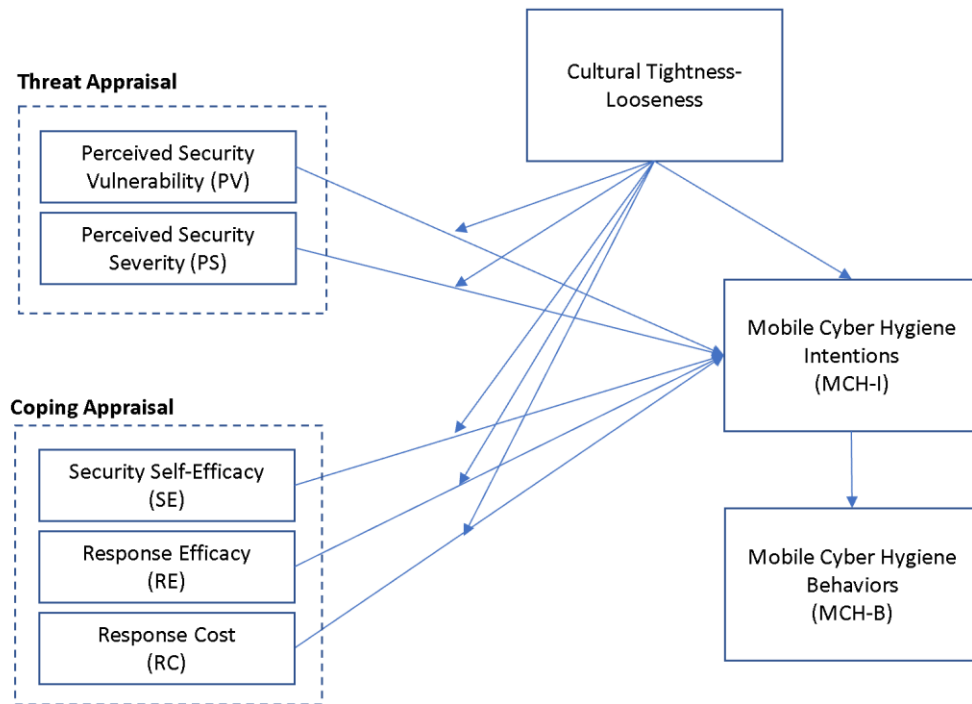


Figure 2 Research Model and Hypotheses

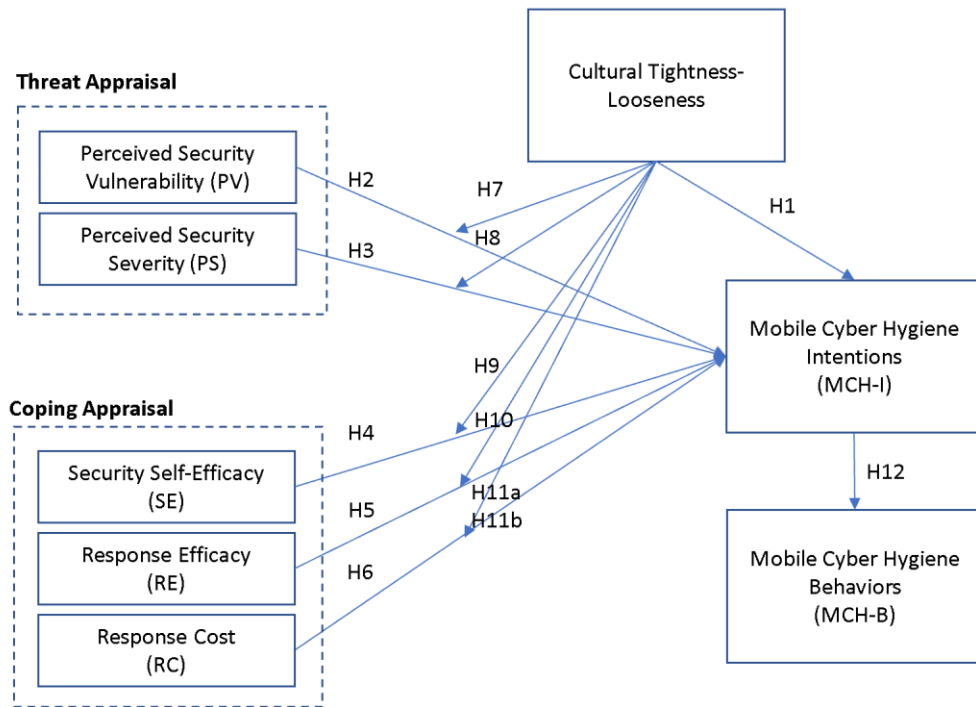


Figure 3 Margin Plot of Cultural Tightness Moderated with Perceived Security Severity

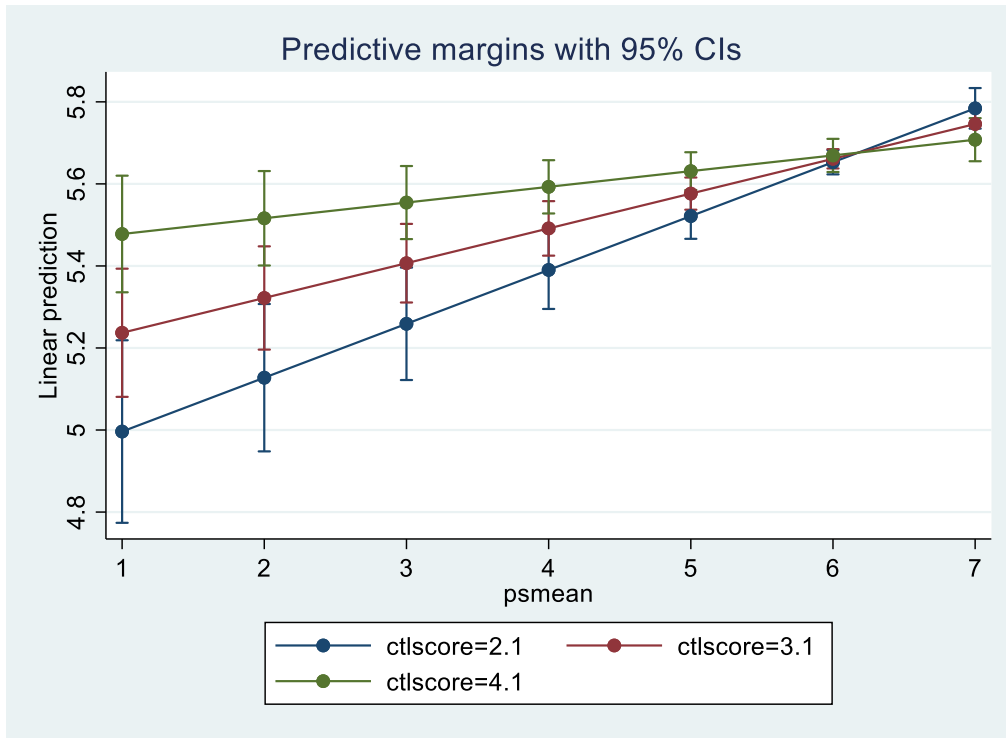


Figure 4 Margin Plot of Cultural Tightness moderated with Response Cost

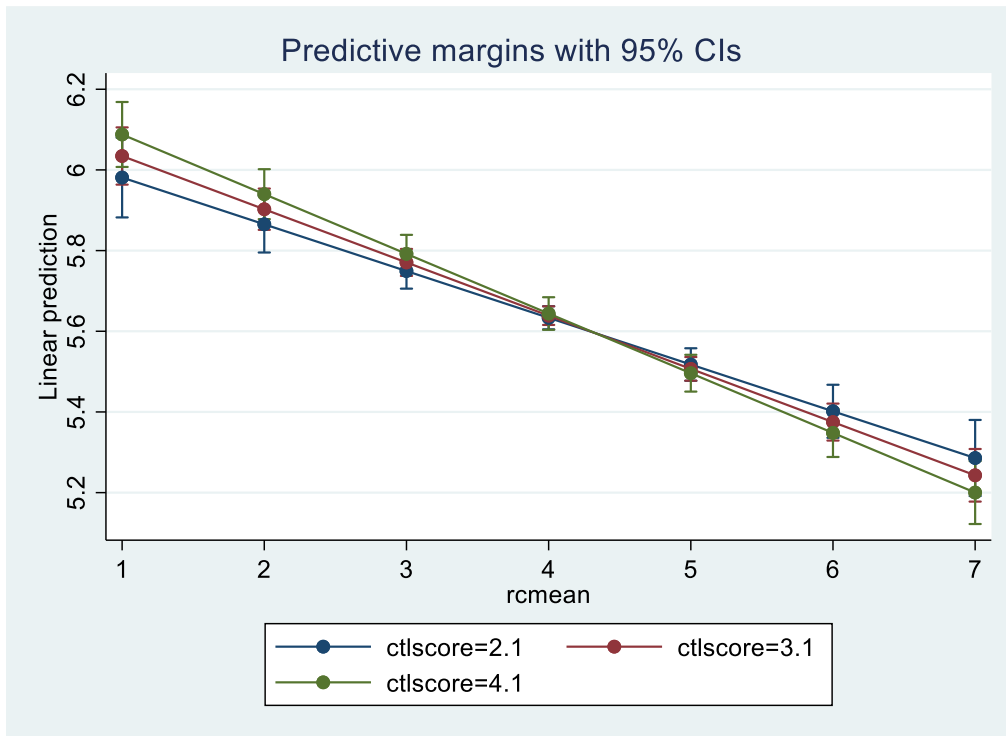


Figure 5 Regression Results

