Cultural and Psychological Factors in Cyber-Security

Tzipora Halevi, Nasir Memon and James Lewis
NYU Tandon School of Engineering
Brooklyn, NY *

Ponnurangam Kumaraguru, Sumit Arora and Nikita Dagar
Indraprastha Institute of Information Technology
New Delhi, India †

Fadi Aloul
American University of Sharjah
United Arab Emirates ‡

Jay Chen
New York University
Abu Dhabi §

ABSTRACT

Increasing cyber-security presents an ongoing challenge to security professionals. Research continuously suggests that online users are a weak link in information security. This research explores the relationship between cyber-security and cultural, personality and demographic variables .

This study was conducted in four different countries and presents a multi-cultural view of cyber-security. In particular, it looks at how behavior, self-efficacy and privacy attitude are affected by culture compared to other psychological and demographics variables (such as gender and computer expertise). It also examines what kind of data people tend to share online and how culture affects these choices.

This work supports the idea of developing personality based UI design to increase users' cyber-security. Its results show that certain personality traits affect the user cyber-security related behavior across different cultures, which further reinforces their contribution compared to cultural effects.

Keywords

Cyber-Security, Culture, Personality Traits, Privacy, Human Factors.

1. INTRODUCTION

*thalevi@nyu.edu,memon@nyu.edu, jpl366@nyu.edu
†pk@iiitd.ac.in, sumitaror@gmail.com, nikita09030@iiitd.ac.in
‡faloul@aus.edu
§jay.chen@nyu.edu

iiWAS '16, November 28-30, 2016, Singapore, Singapore

DOI: http://dx.doi.org/10.1145/3011141.3011165

Online threats continue to be a growing concern. Current systems are designed for the general audience, without regard to differences in its users' personalities. This work suggests approaching applications and system design from user targeted perspective. In particular, understanding the factors that contribute to secure online behavior is an important step towards creating such tailored defenses systems. This research looks at cyber-security behavior, users' self-efficacy (confidence in their ability to mitigate cyber-security risks) and privacy attitude. It examines the relationship between these variables, culture, personality traits and demographic variables (such as gender and computer expertise). It includes participants recruited from four countries and provides a diversified view into the predictors of the examined cyber-security related variables.

The questions this study attempts to answer are the following:

- Is it possible to create a model for participants' secure behavior, self-efficacy and privacy attitude that is based on the users' culture as well as personality?
- How do other factors, such as gender, risk perception and computer expertise affect those parameters?
- How much does culture affect online privacy, sharing of personal information and trust?

1.1 Motivation

Cyber-security threats have been expanding, resulting in a growing number of successful attacks. A recent analysis by Verizon has shown that roughly 90% of successful data breaches were due to users choosing weak or default passwords [14]. The number of attacks from infected websites have also grown significantly in the last few years ($<$ 1 million attacks according to Kaspersky Lab data [13]).

Social engineering scams are based on targeting and manipulating potential victims by appealing to specific human weaknesses. A similar approach also exists for cyber-attacks, ranging from phishing emails [10] to malware attacks [16]. This work makes the argument that the next step in improving overall cyber-security needs to take into account the personality attributes of online users that contribute to the users' decision making under uncertainty. Another factor that may be considered for improving cyber-defenses

is system and software localization. Cultural differences have been shown to affect decision making [4], and examining how these factors affect cyber-security may help improve the future design of cyber-security defenses.

The remainder of the paper is organized as follows: The proposed approach, paper contributions and an overview of related work are presented in sections II, III and IV. The experiments are defined in section V, followed by the results (sections VI, VII and VIII). The paper concludes with section IX.

2. RELATED WORK

Recently, studies began to look at the relationship between decision making, user behavior and personality traits.

Studies by Nov et al. [17, 18] examined the relationship between certain personality traits and the participants response to UI technical cues. The studies make the case that a personality driven UI design can be more effective than a standard design that targets equally the entire user population. In [12], Kajzer et al. examined the effectiveness of security awareness message themes on participants with different levels of personality traits, finding that certain traits make individuals more receptive to security awareness messages.

Another study by Chen et al. [3], looked at how users make decisions involving computer security and risks. It also looked at the contribution of culture, and found that both computer skills and culture have an effect on decision making when asked to assess taking computer security risks vs. monetary rewards.

Slovic et al. [20] considered the perception of risk and how it affects the individual's fear and reaction to certain events. They show that different parts of the population perceive the risks for specific events differently, based on their familiarity with the events and their overall education. In [24], Sleeper et al. studied how users' desire for behavior change on social networks can help design tools for helping users achieve these goals.

Hofstede [1] conducted research into the role of culture across different facets, including uncertainty avoidance in the workplace. While India and USA rank in the lower half, Ghana and the UAE rank in the upper half for this model. People with high uncertainty avoidance may put a higher value on maintaining good security practices and avoid behavior that may seem risky.

Other studies that compared attitudes in different cultures include a study by Shea [11], that compared the attitude towards right to privacy in India and US. As the study pointed out, India is a collective society, and therefore Indians tend to be more trusting of one another. As a result, a significantly larger percent of US respondents were concerned with ID theft relatively to a much smaller percentage of Indian respondents. In addition, [22] and [19] studied different aspects of privacy attitudes in India and US and found that US and Indian participants have different views and concerns. These studies indicate that while multiple cultures may exist in a single country, the differences between those countries are still worth exploring as a whole. In particular, it may result in valuable findings that can be used for future deployment of intercultural systems.

Gender has been studied as a factor in privacy attitude by Facebook users by Mathiyalakan et al. [21], who found differences between their perception of Facebook privacy and overall internet privacy. In [9], differences were also found related to phishing respones. These studies show that gender may indeed play a factor toward both cyber-attitude as well as online behavior. In [8], differences between CS professionals and other study participants were also found to be related to willingness to share fingerprints with online entities, suggesting this may also be a contributing factor in cyber-security related decisions.

3. OVERVIEW OF CONTRIBUTIONS

This research examines the factors that affect different security and privacy-related variables: attitude, behavior and self-efficacy. It took place in a few different countries: US, India, UAE and Ghana. This study shows that while culture is a predictor of privacy attitude, it does not significantly predict self-efficacy and computer secure behavior. It detected a limited correlation between security behavior, self-efficacy and privacy attitude, and found that personality and demographics variables (including gender and computer expertise) affect differently each of those parameters. These findings support the notion that cyber-design should consider the user personality when designing defense system, as personality traits were found to be a significant factor in predicting the user behavior across the different cultures. This work also explores cultural and gender-based differences in online activities, showing that certain activities are more common in certain cultures. One of its findings is that different levels of gender-based self-efficacy exist in different countries.

4. THE PROPOSED APPROACH

The main challenge in defining a new framework for researching human-behavior is creating a model that can be used to assess the relevant aspects. This research starts by defining a few variables related to both handling cyber-security threats as well as 'routine' security behavior. Another aspect that is of interest is the attitude towards privacy. Since the internet poses a large risk to the personal privacy of its users, examining how their attitude relates to their behavior is an important factor.

To assess the variables that affect human behavior, this research adopts the Big-Five Framework, which has been shown to provide a sturdy model of human response and attitude towards encountered events. Another factor that is examined is risk perception, measured through the availability heuristics, which was shown by Tversky &Kahneman [25] to influence decision making under uncertainty. Lately, Schneier [23] has further pointed to the fact that the availability heuristic leads to allocating resources for dealing with specific threats that are not proportional to the consequences (and level of damage) of those threats. General computer expertise was also added as a variable - as it was shown to neutralize the influence of other effects in experts [6]. This variable is measured through examining participants‘ majoring in computer science vs. the other participants. The approach can be viewed in Figure 1.

4.1 Cyber-security and Privacy Framework

Three variables were chosen to match the study objectives. Following are their conceptual definitions:

- **Secure Behavior:** This parameter measures the secure behavior of users online.
- **Self-Efficacy:** This parameter measures the user's confidence in his ability to mitigate cyber-security risks.
- **Privacy Attitude:** This parameter measures how dangerous the users feel it is to share information online.

4.2 Big Five Framework

Personality is a consistent pattern of how people respond to stimuli in their environment and their attitude towards different events. The five factor model of personality assessment is currently one

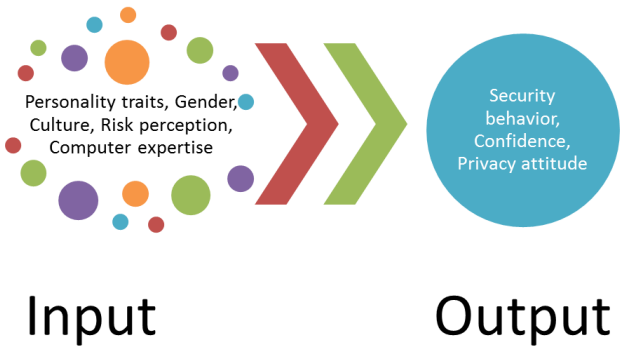

Figure 1: The proposed approach: The input parameters are the personality traits, gender and culture. The output parameters are cyber-security behavior, self-efficacy and privacy attitude

of the most widely used multidimensional measures of personality [15]. Its goal is to encapsulate personality into five distinct factors which allow a theoretical conceptualization of people's personality. These dimensions are Neuroticism, Extroversion, Openness, Agreeableness, and Conscientiousness. Following is a short description of the five traits:

- **Neuroticism:** Neuroticism indicates a tendency to experience negative feelings that include guilt, disgust, anger, fear and sadness.
- **Extroversion:** Extrovert people are more friendly and outgoing and interact more with the people around them.
- **Openness:** Openness indicates the willingness to try new experiences. Openness is also sometimes referred to as 'intellect' and is indicative of general intelligence.
- **Agreeableness:** Agreeable people are co-operative, kind, eager to help other people and believe in reciprocity. They tend to trust other people and believe they are honest and decent.
- **Conscientiousness:** Conscientious people have high self-control and are more organized. They are typically purposeful, strong-minded and tend to be dependable and hardworking

One of the most widely used measures of this five factor model is the NEO-PI FFM test [5]. This is a short 60-questions survey developed by Costa and McCrae that allows for relatively quick, reliable, and accurate measurement of participants personality across these five major dimensions. The framework has been identified as a robust model for understanding the relationship between personality and various academic behaviors. This research sets to examine if this relationship extends to online security and privacy-related behavior.

5. OVERVIEW OF THE SURVEYS

5.1 Methodology

This study took place in four countries: United States, India, UAE (Sharjah) and Ghana. There were 154 participants in the states, 100 participants in India (3 were removed due to partial responses so only 97 results were used), 325 from the UAE and 42 from Ghana. The participants were asked to fill out a survey. In the states, a $10 gift certificate was promised to participants who completed the survey. In India and Ghana, a small compensation was also provided to participants. In the UAE, all the participants were entered in a raffle to win an Ipad.

The survey was hosted on the SurveyGizmo site. Participants were provided the link to the questionnaire. The questionnaire allowed users to stop and go back to the study at a later date.

5.2 Survey

The survey included a demographics questionnaire (such as age, gender, ethnic background, study major etc.). The survey also included the 60-questions NEO-FFM five-factor personality traits survey.

Survey instruments were created for this study to measure the risk perception variable (Availability) and the cyber-security variables. The study constructs are provided in [2]. For the self-efficacy and the cyber-secure behavior, the overall variable was calculated as the sum of all the response values in each construct.

5.2.1 Cyber-Security Constructs - Reliability Test

The constructs created for the cyber-security behavior and the self-efficacy included multiple questions. To measure the self-efficacy the survey asked a series of questions that relate to different risks online, such as viruses, social engineering attacks, internet attacks and fraudulent requests for money. A reliability analysis was performed on the questionnaire results, which produced a Cronbach's value of 0.956, indicating a very high level of internal consistency for this construct.

To measure cyber-security behavior, the survey included questions related to types of data disclosed online, download practices (how often do users download data from unknown sites), password changing frequency, choices of passwords (hard passwords vs. regular passwords) and downloading practices. A reliability analysis was performed oh this construct as well, producing a Cronbach's value of 0.611, which indicates a medium-high level of internal consistency for this construct.

The self-efficacy and the cyber-security behavior were the only constructs that included multiple questions created especially for this study and therefore were tested for reliability (see [2] for the full study). Their relatively high value suggests that these studies indeed were able to measure the intended facets, while providing stable and consistent results.

5.3 Pre-Processing

The goal of this study is to look at the relationship between overall levels of human behavior in cyber-security, self-efficacy, privacy attitude and the different input variables. To achieve this, and reduce the effect of noise on the output parameters – the cyber-security self-efficacy, behavior and privacy attitude variables – the participants were divided into two groups for each variable. Each group included participants with either a high or a low level of the corresponding traits (the groups were divided using the mean of each parameter).

As part of the input variables a 'CS major' variable was created (to mark if the study major was CS). This included participants that

studied both computer science as well as computer engineering (the responses did not include any participants who stated their major as 'information system' or 'MIS', nor any other participants who were computer professionals, who would have also qualified to be considered to be in this group). For the countries, nominal values were defined. All of the input parameters were normalized between 0 and 1. The calculations were carried using the SPSS software.

6. FACTORS THAT INFLUENCE SECURITY AND PRIVACY

6.1 Relationship between the variables

Security Parameters.

Examining the correlation between the variables, this study finds that while secure behavior and self-efficacy are correlated, the correlation is only moderate. It also finds that privacy attitude has low correlation to the other two variables. This suggests that different factors contribute to the ability to predict behavior of subjects, ability to handle security-related activities and the user's privacy attitude.

	Behavior	Self-efficacy	Privacy Attitude
Secure Behavior	1	.296**	-.031
Security self-efficacy	.296**	1	.067
Privacy Attitude	.031	.067	1

** - Correlation is significant at the 0.001 level (2-tailed).

Table 1: Correlation between Cyber-security variables. There is a medium correlation between self-efficacy and secure behavior. There is no significant correlation between privacy attitude and the other tested variables.

Gender and Major.

The statistics for this study showed that (for its participants) there was no correlation between being a CS major and gender. Overall, 23% of the participants were CS major, with 24% of the men and 21% of the women being CS students. When calculating the correlation, these variables were found to be statistically independent.

Major and Personality Traits.

The only correlation found between those variables was a low negative correlation (-0.093) between conscientiousness and computer science major (with $p < 0.05$). Overall, this study suggests that being computer science major students is not significantly correlated to conscientiousness .

6.2 What contributes to secure behavior, self-efficacy and privacy attitude?

To examine the contribution of the different factors, a binary logistic regression was performed on the normalized variables. The impact of each of the independent variables was tested on each of the three security-defined parameters.

The personality traits of extraversion and agreeableness were not found to be significantly correlated to any of the variables and were removed. The results appear in Tables 2, 3 and 4 (all of the three models are statistically significant at $p < 0.001$).

Following are observations for the study findings:

Culture: Culture was found to be a significant predictor of privacy attitude. It had a low effect on behavior (at $p < 0.1$), and was not a predictor of self-efficacy. This shows that while culture does affect privacy attitude, global factors may contribute more to behavior and self-efficacy.

Personality Traits: Conscientiousness was found to be a significant predictor of behavior. This indicates that hard-working and detailed-oriented participants also tend to be more secure in their online behavior. Openness to experiences, which also indicates intelligence, was found to be a strong predictor of self-efficacy. On the other hand Neuroticism was found to be inversely correlated to self-efficacy (at $p < 0.1$). This shows that emotional stability (the inverse of Neuroticism) can predict a positive self-efficacy. Personality traits were not found to significantly predict privacy attitude, showing that culture, demographics and risk perception tend to predict user's privacy attitude.

Risk Perception: Risk perception predicts both secure behavior as well as self-efficacy. This suggests that people who have higher risk perception and are familiarity with previous attacks may be likely to practice secure behavior and develop a higher confidence in their ability to mitigate security risks. Participants with higher risk perception were also found to have higher privacy attitude.

Gender: Gender was found to be a strong predictor of self-efficacy, with men feeling more confident in their ability to mitigate cyber-security risks. However, it was not found to be a strong predictor of behavior. Gender was also found to be an inverse predictor of privacy attitude, which indicated that men perceived having a higher privacy attitude online.

CS Major: Studying CS was found to be a significant predictor of both secure behavior as well as of self-efficacy, with a higher effect on self-efficacy. However, it was not found to be correlated to privacy attitude.

	B	S.E.	Wald	Sig
Neuroticism	-.457	.632	.523	.470
Openness	1.269	.714	3.158	.076
Conscientiousness	1.859**	.619	9.025	.003
risk perception	.413*	.178	5.396	.020
Gender	.095	.195	.237	.6273
CS Major	.600**	.201	8.901	.003
culture	-.550	.309	3.179	.075

$*p \leq 0.05, **p \leq 0.01, ***p \leq 0.001$

Table 2: Logistic Regression of Secure Behavior Variable. Conscientiousness is the major factors for predicting secure behavior. Other predictors to secure behavior are previous exposure to vulnerabilities and being a CS major.

6.2.1 Discussion

Culture was found to be a predictor of privacy attitude, but only had low effect on behavior and was not found to predict self-efficacy. This supports the idea that cyber-security-defenses can be developed globally and may consider to a large extent other variables, such as personality and demographics variables.

When examining the contribution of the personality traits to predicting the cyber-security related variables, openness was found to be a higher predictor of self-efficacy related to handling security

	B	S.E.	Wald	Sig
Neuroticism	-1.154	.681	2.871	.090
Openness	2.076**	.763	7.392	.007
Conscientiousness	.733	.638	1.320	.251
risk perception	.453*	.193	5.529	.019
Gender	1.292***	.215	36.112	.000
CS Major	1.458***	.234	38.895	.000
culture	.301	.331	.831	.362

$*p \leq 0.05, **p \leq 0.01, ***p \leq 0.001$

Table 3: Logistic Regression of Cyber-security self-efficacy. Openness is the major factor. Other factors that affect self-efficacy are gender as well as being a CS major

	B	S.E.	Wald	Sig
Neuroticism	.320	.687	.217	.642
Openness	-.630	.778	.655	.418
Conscientiousness	.515	.670	.590	.442
risk perception	.408*	.205	3.941	.047
Gender	-.630**	.231	7.431	.006
CS Major	-.183	.220	.692	.406
culture	2.335***	.394	35.127	.000

$*p \leq 0.05, **p \leq 0.01, ***p \leq 0.001$

Table 4: Logistic Regression of Privacy Attitude Variable. Culture is the largest predictor of privacy attitude, as well as gender and risk perception (knowledge of previous cases of internet misuses). Personality parameters were not found to be significant predictors of this variable

than for secure behavior. However, it is a significant factor for both (at $p < 0.1$). While openness has been previously shown to be a major contributor to academic achievement [26], this study showed it may also contribute to secure behavior and confidence. Another personality factor, conscientiousness, is shown to be a strong predictor of behavior but not of self-efficacy. On the other hand, emotional stability (the inverse of neuroticism) was found to be a predictor of self-efficacy (at $p < 0.1$), but did not significantly predict the participant's behavior. These differences may suggest potential reasons for the limited correlation between behavior and self-efficacy.

Major and gender also had different effects on those variables, with men found to be more confident about their abilities to solve security-related issues. Being a CS major is also a major contributor to self-efficacy. However, the major has a much smaller contribution to the behavior of the participants, while the gender does not have significant contribution. This shows that while education affects significantly the self-efficacy related to handling different vulnerabilities and events, it may affect less the daily overall online users' behavior. Also, while women are less confident of their abilities, there is no significant difference in their actual cyber-security behavior.

One of the study limitations is due to the fact that most of the participants in it were students (90% of the participants). Therefore future studies are recommended that will use different demographics, which may be able to detect additional factors relating to profession and security attitude.

Risk perception was found to be a significant factor for all the parameters. This shows that computer users who are familiar with previous attacks tend to be risk averse and will put a higher priority on security and privacy.

Overall, these results suggest that personality and risk perception are important factors in behavior and therefore understanding them can help improve system design targeted at increasing the secure behavior of online users.

7. CULTURAL DIFFERENCES - SELF-EFFICACY AND GENDER

This study further examines the relationship between culture, self-efficacy and gender. To study those, self-efficacy was examined as a function of both culture and gender simultaneously.

While culture was not found to be a significant predictor of cyber-security-related self-efficacy in this study, gender-based differences related to self-efficacy were found between the countries. Since the Ghana study only included six women (and thirty six men), the Ghana data was excluded for this part of the study, and only the US, UAE and India data was used. This study found that in the states, self-efficacy difference is larger between the genders compared to participants from UAE and India. The results can be seen in Table 5 and Figure 2. These findings show that cyber-security risks are perceived similarly to other offline risks. In [7], Finucane et al. state that 'risks tend to be judged lower by men than women and by white people than by people of colour'. This study finds that self-efficacy, which is the perceived ability to handle those risks, is higher on average for US men relatively to all the other participants. This is a preliminary finding (due to the relatively limited number of participants from each country) and would be interesting to study in a larger diversified population in the future.

culture	Gender	Mean	No. of Participants
U.S.	Men	.77	111
U.S.	Women	.16	43
UAE	Men	.49	241
UAE	Women	.26	84
INDIA	Men	.74	70
INDIA	Women	.68	28

Table 5: Comparison of the mean values of self-efficacy as related to gender and culture. This study showed that in the USA, the difference was the largest as a factor of gender, followed by UAE and India

8. ONLINE INFORMATION SHARING ACROSS DIFFERENT CULTURES

This study further examined different online activities across cultures. To that end, the participants were asked about the type of personal information that they tend to share online. Overall, US participants were found to share more information online than participants form other countries (See Table 6). This study also shows that while online banking is popular in the US, it is still less popular in other cultures. As the trend of online banking grows, this may also raise the potential for online attacks in new regions.

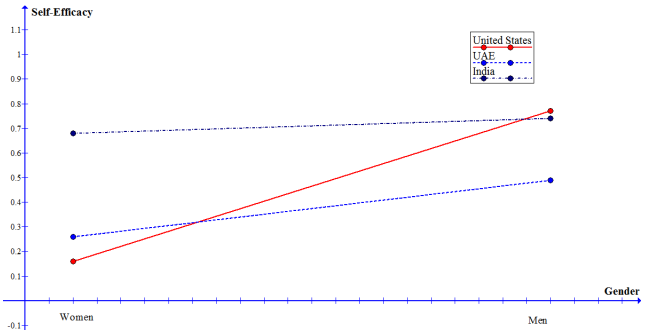

Figure 2: Security-related self-efficacy as a function of culture and gender. This study shows that gender has a higher effect on the self-efficacy level in the United States (represented by the red line) and a lower effect in India (green line) and UAE (blue line)

	USA	UAE	India	Ghana
Online Banking	0.72	0.38	0.64	0.43
Entering Credit Card data	0.59	0.40	0.44	0.30
Allow Saving CC Data	0.56	0.33	0.32	0.29
M. Maiden N.	0.59	0.46	0.48	0.46
Birth Date	0.63	0.76	0.64	0.64
Address	0.60	0.56	0.52	0.61
Workplace	0.59	0.57	0.57	0.54
Medical Info	0.54	0.44	0.43	0.43

Table 6: Comparison of the mean values of online information sharing parameters across the different locations. People in USA are the most trusting, while people in Ghana are the least trusting, with the other countries in between.

Surprisingly, the participants from the states were found to be more comfortable sharing their mother's maiden name online than the participants from the other countries, even though this data is often used as a form of identification when contacting US banks and financial institutions. Another finding is that birth-date was not viewed as very sensitive data. This is especially true in UAE, where participants indicated most would be willing to share it online.

Birth-date, address and workplace variables were found not to be statistically correlated to culture. Sharing credit card and medical information were found to be correlated with culture, as well as online banking (at $p < 0.05$). The highest correlation to culture was storing credit card information ($r = 0.42$), followed by sharing credit card information ($r = 0.39$). Mother's maiden name, medical information and online banking had lower significant correlation, with ($r = 0.2, p < 0.01$). It was interesting to see that USA participants were less private than their counter parts regarding sharing of credit card information. This is likely due to the insurance that US credit card companies provide to their users.

However, the fact that people on average share their mother's maiden name more than their credit card information was unexpected, as this data can be used for authentication. Similarly, the general high level of sharing of birth-date (which was higher than credit card information sharing in all countries) is also surprising and may lead to identity theft. This implies that participants do not distinguish between data that can be changed (such as credit card information, which can be changed by canceling the card) and permanent data (such as birth date and mother's maiden name). These findings suggest it may be beneficial to educate customers about the risks in revealing different types of data, emphasizing the potential dangers in sharing permanent data online. raising participants' sensitivity to sharing permanent data online.

9. CONCLUSIONS AND FUTURE RESEARCH

This research presents the idea of creating a framework for characterizing participants' cyber-security behavior that takes into account the culture and user personality. To explore this idea, it develops instruments to measure the participants routine cyber-security behavior and their self-efficacy in handling security-related threats online and examines the factors that affect those measured parameters.

This is the first study that the authors are aware of that looks at the contribution of culture vs. personality on users' cyber-security behavior, self-efficacy and privacy attitude. It shows security trends in different countries.

This study found that while culture significantly predicts privacy attitude, security-related behavior and self-efficacy were not affected significantly by this variable. While there are differences in online behavior, other factors, such as specific personality traits, demographics and education are better predictors of security behavior and self-efficacy. Another observation was that gender affects participants self-efficacy, with men having higher confidence in their abilities. The largest difference based on gender was found in the US. However, gender was not found to affect significantly the security-related behavior of the participants.

The findings suggest certain trends in security behavior and perception, which support taking a global approach for developing security-related systems, geared towards the personality characteristics and demographic information of the users. It further suggests that cross-cultural research may be beneficial as different countries share similar concerns regarding cyber-security. Future work should concentrate on presenting specific design interventions based on the users' personality traits and their risk perception and explore how those may help increase users' secure behavior online.

10. ACKNOWLEDGMENTS

This work was supported in part by the NSF (under grant 0966187). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

The authors would also like to express their thanks to all members of Precog research group at IIIT - Delhi.

11. REFERENCES

[1] Strategy-culture-change. https://geert-hofstede.com/countries.html.

[2] Survey Instrument. http://bit.ly/1Y3jDpc.

[3] L.-C. Chen and D. Farkas. An Investigation of Decision-Making and the Tradeoffs involving Computer Security Risk. *proceeding of: Proceedings of the 15th Americas Conference on Information Systems*, (610), 2009.

[4] P. Chua, E. E. Spiresa, and T. Sueyoshi. Cross-Cultural Differences in Choice Behavior and Use of Decision Aids: A Comparison of Japan and the United States . *Organizational Behavior and Human Decision Processes*, pages 147–170, 1999.

[5] P. Costa and R. R. McCrae. *NEO PI-R professional manual*. Psychological Assessment Resources, Inc, Odessa, FL, 1992.

[6] B. Englich and K. Soder. Moody experts - How mood and expertise influence judgmental anchoring. *Judgment and Decision Making*, 4(1):41 – 50, February 2009.

[7] M. L. Finucane, P. Slovic, C. K. Mertz, J. Flynn, and T. A. Satterfield. Gender, race, and perceived risk: The 'white male' effect. *Health, Risk & Society*, 2(2):159–172, 2000.

[8] T. Halevi, T. Kuppusamy, M. Caiazzo, and N. Memon. Investigating users' readiness to trade-off biometric fingerprint data. *IEEE Internation Conference on Identity, Security and Behavior Analysis (ISBA)*, 2015.

[9] T. Halevi, J. Lewis, and N. Memon. A pilot study of cyber security and privacy related behavior and personality traits. *WWW '13 Companion Proceedings of the 22nd international conference on World Wide Web companion*, pages 737–744, 2013.

[10] M. Jakobsson and S. Myers. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience, December 2006.

[11] Jane Hill Shea. Attitudes Toward Privacy: A Comparison of India and the United States. http://www.frostbrowntodd.com/resources-214.html, 2007.

[12] M. Kajzer, J. DArcy, C. Crowel, and D. V. Bruggen. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43:64 – 76, 2014.

[13] R. Lemos. Kaspersky Security Bulletin 2013. Overall statistics for 2013. https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013#07, 2013.

[14] R. Lemos. Targeted Attacks, Weak Passwords Top IT Security Risks in 2013. http://www.eweek.com/security/targeted-attacks-weak-passwords-top-it-security-risks-in-2013/, 2013.

[15] R. R. McCrae and O. P. John. An Introduction to the Five-Factor Model and Its Applications. *Journal of Personality*, 60(2):175 – 215, June 1992.

[16] Microsoft. Zeroing In on Malware Propagation Methods. *Microsoft Security Intelligence Report*, 11, May 2011.

[17] O. Nov and O. Arazy. An Investigation of Decision-Making and the Tradeoffs involving Computer Security Risk. *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 977–984, 2013.

[18] O. Nov, O. Arazy, C. Lopez, and P. Brusilovsky. Exploring personality-targeted UI design in online social participation systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 361–370, 2013.

[19] P. Kumaraguru and L. F. Cranor and E. Newton. Privacy Perceptions in India and the United States: An Interview Study. http://precog.iiitd.edu.in/Publications_files/tprc_2005_pk_lc_en.pdf, 2005.

[20] Paul Slovic and Elke U. Weber . Perception of Risk Posed by Extreme Events . *Risk Management strategies in an Uncertain World*, 2002.

[21] S. Mathiyalakan and G. Heilman and S. White. Gender Differences in Student Attitude toward Privacy in Facebook . *Communications of the IIMA*, 13(4):34 – 42, 2013.

[22] S. Paril and A. Kosba and A. John and D. Seligmann . Comparing privacy attitudes of knowledge workers in the U.S. and India. *ICIC '10 Proceedings of the 3rd international conference on Intercultural collaboration*, pages 141–150, 2010.

[23] B. Schneier. Fear and the Availability Heuristic. https://www.schneier.com/blog/archives/2009/03/fear_and_the_av.html, 2009.

[24] M. Sleeper, A. Acquisti, L. F. Cranor, P. G. Kelley, S. A. Munsonz, and N. Sadeh. "I Would Like To..., I Shouldn't..., I Wish I...: Exploring Behavior-Change Goals for Social Networking Sites" . *CSCW '15 Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 1058–1069, 2015.

[25] A. Tversky and D. Kahneman. Judgment under Uncertainty: Heuristics and Biases. *Science New Series*, pages 1124–1131, 1974.

[26] A. Zuffiano, G. Alessandri, M. Gerbino, B. P. L. Kanacri, L. D. Giunta, M. Milioni, and G. V. Caprara. Academic achievement: The unique contribution of self-efficacy beliefs in self-regulated learning beyond intelligence, personality traits, and self-esteem. *Learning and Individual Differences*, 2012.