IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 1, January 2016

Gender Differences in Risk Perception of Trust and Bias in Cyberspace

Emeka P. Idoye[1], Eui H. Park[2], Celestine A. Ntuen[3]

Department of Industrial & Systems Engineering, North Carolina Agricultural & Technical State University, Greensboro, USA[1,2,3]

Abstract: This study investigates risk perception related to trust and bias in cyberspace under different levels of cognitive risks. It is hypothesized that risk perception in cyberspace is different by gender and is influenced by trust and bias, as well as by fear and privacy factors. Based on Kahneman & Tversky's [6] study of Prospect Theory, the trust and bias risk quadrants are used to determine how an individual will perceive usage of cyberspace. The objective of this study is to mitigate fear and privacy issues between genders while performing certain activities online. This study was conducted by implementing two phases of surveys. ANOVA and correlation analyses were performed to show the differences in gender and the relationships of the variables in each risk quadrant.Results of this study may help increase trust and reduce negative perceptions of cyberspace by designing better websites and interfaces for users.

Keywords: bias, cyberspace, risk, trust.

I. INTRODUCTION

Cyberspace refers to interconnected networks or the space within which electronic communications take place. Cyberspace is used interchangeable with the Internet and the World Wide Web and their use by the public. As a digital community, people, physical entities and services now share a common work and social space. In cyberspace, objects and entities that interact do not need to be physically present; they do so in a virtual environment. For example, in internet commerce, people are able to receive services that they would normally get in real life physical space [1].

As with every other technology, cyberspace has its bad sides, such as concerns for risk, security, trust, usability, vulnerability, and so on. For instance, for the USA, an attack to any of its cyber infrastructure systems could be catastrophic to the defense or economic security of the country and the world. A report by the Presidential Commission [2] noted that threats to critical national infrastructures fall within two categories: (1) physical threats to tangible properties, and (2) cyber threats which are threats of electronic, radio-frequency or computer-based attacks on the information or communications components that control critical infrastructures. Both types of attacks induce a perception of risk and compromise human trust in system of interests.

Trust in cyberspace is a critical factor for the acceptance of electronic services including those provided by electronic commerce and e-government service providers. Trust is defined as the expectation that the promise of another can be relied upon and in unforeseen circumstances, the other will act in the spirit of goodwill and in a benign fashion toward the trusting party [3].

Positive (Trust): This is the tendency to rely on or believe in some information with optimism. Trusting stance means that regardless of what one assumes about a situation generally, one expects to achieve better outcomes by dealing with the situation as though it is well-meaning and reliable [4].

Negative (Distrust): This is the tendency to avoid reliance or not believe in something due to feeling that an event or artefact cannot be relied on; does not instil confidence, and is highly suspicious and doubtful. [5].

Risk: Risk is the probability of adverse events or consequences (such as loss of privacy or virus attack on computers) resulting from use of a cyber-site [6]. With respect to cyber risks, many factors can be contributors to risk.

Bias: This describes one's tendency to view something from a particular perspective. This perspective prevents the person from being objective and impartial [7]. A bias behavior can be positive or negative. A positive or a negative bias influences an individual to either trust or distrust a cyberspace.

This study of gender differences in risk perception related to trust and bias in cyberspace is important because risk, trust, and bias are relevant in understanding human behaviors using digital information system and their devices. Some examples are how people choose the internet over many other options, use social network sites, or conduct web-based financial and commercial transactions. These behaviors are informed by risks and threats from cyberspace. In this study, it is assumed that trust in cyberspace is a function of perceived fear and privacy and the available information about risk in cyberspace. A survey was designed to collect data about the subject's perception and usage of cyberspace. ANOVA and correlation analysis were performed to show the differences in gender and the strength of relationships of the variables in each risk quadrant.

There are many indications that gender differences exist in risk perceptions of trust and bias in cyberspace. These

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 1, January 2016

differences will be investigated by the risk quadrants based on Kahneman & Tversky's study [6].

Quadrant I represents negative bias and positive trust, indicating a tendency or opportunity for risk seeking behavior due to conflicting information in which the information is tilted towards favorable reports on trust [11]. This quadrant could describe people who trust a cyber-site even though they have information on a high risk. The negative bias is likely to be caused by the available information on perception of high risk consequences.

Quadrant II represents people that have the tendency to exhibit a positive bias and a positive trust in a cyber-site because of the perceived low risk consequence [12].

Quadrant III is where people will distrust a cyber-site even though they tend to be biased positively because of low risk consequences. This could be due to a stereotyped behavior such as in people who do not like to use cyber-site because of fear [13]. Harber and Pennebaker [14] note that when people develop negative viewpoints about an object or a situation, it is difficult to alter those viewpoints.

Quadrant IV represents both negative bias and distrust. Here, it is argued that people who have experience with consequences of high risk leading to a negative bias are likely to distrust a cyber-site [15].

A trust scale that overlaps a bias scale is used to describe the trust-bias quadrants as shown in Figure 1. A fear scale that overlaps a privacy scale is used to describe the fear-privacy quadrants as shown in Figure 2.

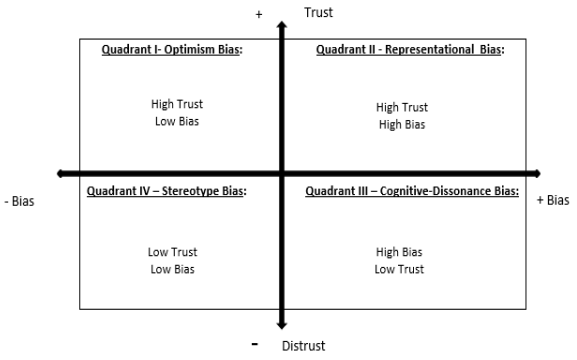

Fig. 1 Trust-Bias Risk Quadrants

Quadrant I: (Optimism Bias)
H_0: There is no significant difference in gender on risk perception of high trust and high bias in cyberspace.

Quadrant II: (Representational Bias)
H_0: There is no significant difference in gender on risk perception of low trust (distrust) and highbias in cyberspace.

Quadrant III: (Cognitive-Dissonance Bias)
H_0: There is no significant difference in gender on risk perception of high bias and low trust (distrust) in cyberspace.

Quadrant IV: (Stereotype Bias)
H_0: There is no significant difference in gender in risk perception of low trust (distrust) and low bias in cyberspace

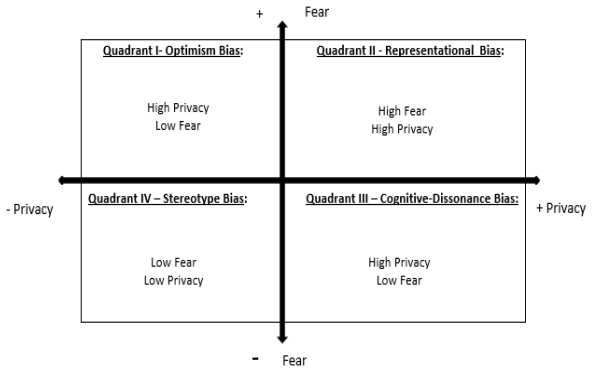

Fig. 2Fear and Privacy Risk Quadrants

Quadrant-I: (Optimism Bias)
H_0: There is no significant relationship in gender on high fear and high privacy in cyberspace.

Quadrant II: (Representational Bias)
H_0: There is no significant relationship in gender on low fear and high privacy in cyberspace.

Quadrant III: (Cognitive-Dissonance Bias)
H_0: There is no significant relationship in gender on high privacy and low fear in cyberspace.

Quadrant IV: (Stereotype Bias)
H_0: There is no significant relationship in gender on low fear and low privacy in cyberspace.

II. MATERIALS AND METHODS

The study consists of two stages. Instrument I, a sample survey questionnaire(shown in Table I)measures fear and privacy in cyberspace. Fear is defined here as an unpleasant emotion caused by the belief that the use of cyberspace is dangerous and is likely to incur cost or some psychological burden. Fear is also a result of an individual's perception of uncertainty about loss or gain in a particular transaction [8]. An example is people who shop online are concerned with the quality of products they will receive and entertain some fear on how their information will be used later. Privacy deals with identity of the user of cyberspace. Users of cyberspace relate risk to their privacy of information [9]. The responses to each fear question are based on a five point Likert scale used in similar studies [10] with the scale: (1) Strongly Disagree, (2) Disagree , (3) Neither agree or Disagree, (4) Agree and,(5) Strongly Agree. The fear questionnaire has twenty 26 factors and privacy questionnaire has 28. Instrument II shown in figure 3 was designed to capture risk perception and also captured the levels of trust or distrust after completing the fear questionnaire.

TABLE I COMPONENTS OF FEAR FACTOR QUESTIONNAIRE FROM QUADRANT I

Quadrant I: The people who fall into this category could describe people who show positive trust in cyberspace even though they know its risks (risk seeking behavior).
FQ11. How concerned are you about somebody impersonating you and shopping under your name?

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 1, January 2016

FQ12. How concerned are you about being monitored on the internet?
FQ13. How concerned are you with cyber-stalking or cyber-harassment?
FQ14. How concerned are you that you might receive a virus that could infect your computer system?
FQ15. How concerned are you about entering your debit or credit card numbers over the internet?
FQ16. How concerned are you that your computer might be accessed / hacked by other users?
FQ17. How concerned are you that you might become a victim of a computer related crime?
FQ18. How concerned are about being a victim of extortion or blackmail via the internet?
FQ19. How likely are you to participate in an online auction for buying a product online?

A reliability test was conducted on the fear and privacy factor questionnaires using Cronbach's criterion. The generally agreed upon lower limit for Cronbach's alpha is 0.70. The results of the exploratory factor analysis were used to identify the number of fear and privacy constructs for inclusion in the risk quadrants.

Participants

The subjects for the study were selected from a population of college students. The student population is known to have vast experience with cyberspace using websites such as Facebook, Twitter, Amazon.com, etc.). Subjects were self-selected and as an incentive for participating in the experiments, subjects received cash prizes. A total of 68 participants, consisting of 34 females and 34 males, participated in the study.

Experimental Procedure and Task

Participants were welcomed into the Human-Machine Systems Laboratory at the university and administered the study's informed consent form. First, the participants completed the fear and privacy questionnaires. Thenthey used the computer for administration of the trust-bias instrument that consisted of four scenarios used as a case study on XYZ website. After reading the scenarios, the subjects used the trust-bias instrument interface (shown in Figure 3) to choose their trust or bias level using the computer scale.

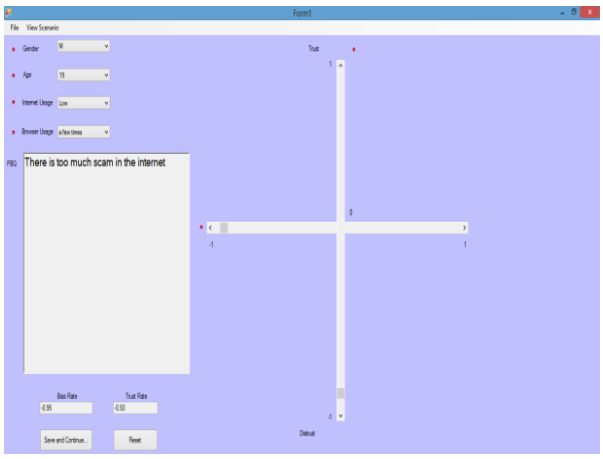

Fig.3. Bias-Trust rating instrument

III. STATISTICAL ANALYSIS

Analysis of Variance (ANOVA) was used to study the perception of trust and distrust based on the fear privacy factors loaded into each risk quadrant by gender. Two sample ANOVA results for trust and bias risk quadrants are shown on figures 4 and 5. Correlation analysis was used to explore the relationships that exist between females and males and to explore the relationships across each of the four risk quadrants.

A sample of quadrant I (Optimism Bias) analysis show the effect of risk perception of trust was statistically significant. The MSE value of 0.135 indicates the average of the difference between the estimator and what is estimated is smaller (p value = ≤0.0110). The female group had a mean of 0.82 trust while the male group had 0.72 respectively.

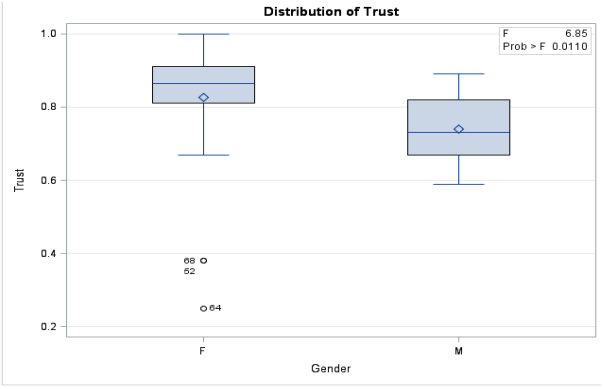

Fig.4. ANOVA for Quadrant I Trust

A sample of quadrant II (Representational Bias) analysis shows the effect of risk perception of bias was also statistically significant. The MSE value of 0.157 indicates the average of the difference between the estimator and what is estimated is smaller (p value = ≤.0001). The female group and male group means for bias were 0.70 and 0.90, respectively.

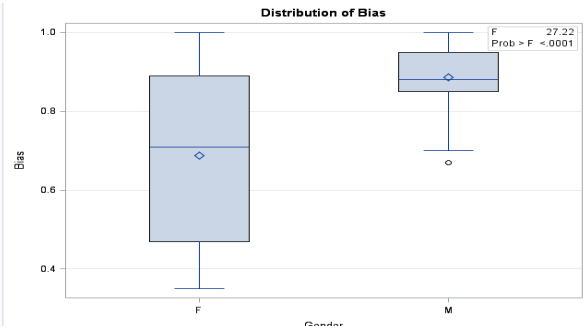

Fig.5. ANOVA for Quadrant II Bias

Correlation analysis was used to explore the relationships between the questions based on trust-bias and fear-privacy factors loaded into each risk quadrant. The variables with strong and very strong relationships were investigated.

The males in Quadrant I of Optimism Bias are prone to exhibit more fear than privacy while performing activities in cyberspace. Females in Quadrant II (Representational

Bias) exhibited more fear than privacy while performing activities in cyberspace. Females in Quadrant I (Optimism Bias) exhibited more privacy than fear while performing activities in cyberspace. Males in Quadrant II (Representational Bias) exhibited more privacy than fear while performing activities in cyberspace. Females in Quadrant IV of Stereotype Bias exhibited more privacy than fear while performing activities in cyberspace.

Results

I. Gender differences in risk perception of trust and bias in cyberspace from the fear factors are: 1) Bias in Quadrant I (Optimism Bias), the female group showed more bias compared to the male group and was significant. The null hypothesis was not rejected. 2)Trust in Quadrant I (Optimism Bias) for fear factors, the female group showed more trust compared to the male group and was significant. The null hypothesis was not rejected.
3) Bias in Quadrant II (Representational Bias), the male group showed more bias compared to the female group and was significant. The null hypothesis was not rejected.4) Trust in Quadrant II (Representational Bias), the male group showed more trust compared to the female group and was significant. The null hypothesis was not rejected.
5) Bias in Quadrant III (Cognitive-Dissonance Bias), the male group showed more bias compared to the female group and was significant. The null hypothesis was rejected.6) Trust in Quadrant III (Cognitive-Dissonance Bias), the male group showed more distrust compared to the female group and was significant. The null hypothesis was rejected.7) Bias in Quadrant IV (Stereotype Bias), the male group showed more negative bias compared to the female group and was significant. The null hypothesis was rejected. 8) Trust in Quadrant IV (Stereotype Bias), the male group showed more distrust compared to the female group and was significant. The null hypothesis was rejected.

II. Gender differences in risk perception of trust and bias in cyberspace from privacy factors are: 1) Quadrant I (Optimism Bias), the female group showed more bias compared to the male group and was not significant. The null hypothesis was rejected. 2) Quadrant I (Optimism Bias), the female group showed more trust compared to the male group and was not significant and the null hypothesis was not rejected. 3) Bias in Quadrant II (Representational Bias), the male group showed more bias compared to the female group and was significant. The null hypothesis was not rejected. 4) Trust in Quadrant II (Representational Bias), the male group showed more trust compared to the female group and was significant. The null hypothesis was not rejected. 5) Bias in Quadrant III (Cognitive-Dissonance Bias), the male group showed more bias compared to the female group and was significant. The null hypothesis was not rejected.6) Trust in Quadrant III (Cognitive-Dissonance Bias), the male group showed more distrust compared to the female group and was significant. The null hypothesis was not rejected.
7). Bias in Quadrant IV (Stereotype Bias), the male group showed more negative bias compared to the female group and was significant. The null hypothesis was not rejected.8). Trust in Quadrant IV (Stereotype Bias), the male group showed more distrust compared to the female group and was significant. The null hypothesis was not rejected.

III. The correlation analysis of fear and privacy factors for female and male groups is as follows. 1) Males in Quadrant I (Optimism Bias) exhibited more fear than privacy while performing activities on cyberspace. 2) Females in Quadrant II (Representational Bias) exhibited more fear than privacy while performing activities in cyberspace. 3) Females in Quadrant I of (Optimism Bias) exhibited more privacy than fear while performing activities in cyberspace.4) Males in Quadrant II (Representational Bias) exhibited more privacy than fear while performing activities on cyberspace. 5) Females in Quadrant IV of (Stereotype Bias) exhibited more privacy than fear while performing activities on cyberspace.

IV. CONCLUSION

In this study females showed more bias behavior and trusting behavior for fear and privacy factors. This showed that women are more comfortable in using cyberspace casually for activities such as email, online shopping, social media, and sharing some personal information online. Men showed some bias behavior and some others did not for fear and privacy factors and some did not trust using cyberspace. This showed that men are also comfortable performing certain activities in cyberspace, but are not comfortable performing some tasks such as buying a product online from a seller with low ratings, fearing that they might be scammed or sold a counterfeit product.

The correlation analysis showed women exhibit both fear and privacy while performing activities on cyberspace.
The correlation analysis also showed that men exhibit more of a privacy behavior than fear while performing activities in cyberspace. The correlation analysis also showed that men exhibit more privacy behavior than fear while performing activities in cyberspace. The analysis was performed on each of the four quadrants for fear and privacy factors that looked at significant variables. The strength of the correlated variables was also investigated to the strength of the relationship of the variables.

Some challenges in conducting this research was in developing and validating acceptable fear and privacy factors that capture people's perception of using cyberspace. The present findings are also subject to limitations. This study may not give a true representation of the user's perception of cyberspace due to the demographics of the study.

The results from this research indicate that providing assurance by mitigating negative perceptions is the key in developing trust relationships with cyberspace users. The results of this research are important to internet and website designers and users in terms of considering different levels of risk in design that will increase trust of patronage.

ACKNOWLEDGMENT

Emeka P. Idoye wishes to acknowledge all survey participants which made this study possible.

REFERENCES

[1] Mai, H. N., Pymont, D., Shen W., Z., & Zhang, C. X. (2007). Managing the Digital Enterprise Trust in Cyberspace.
[2] Infrastructures, C.F.P.A. s. (1997). The Report of the President's Commission on Critical Infrastructure Protection. Washington, DC.
[3] Bhattacherjee, A. (2000). Acceptance of E-commerce services: The case of electronic brokerages. IEEE Trans on Systems, Man and Cybernetics---Part A: Systems and Humans, 30(4), 411-430.
[4] Sitkin, S. B., & Roth, N. L. (1993). Explaning the limited effectiveness of legalistic "remedies for trust/distrust. Organization science, 4(3), 367-392.
[5] Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. Journal of consumer research, 119-134.
[6] Kahneman, D & Tversky, A. (1979). Prospect theory: An analysis of choice Under Risk. Econometrica, 47(2), pp. 263-291.
[7] Evans, J. S. B. (1989). Bias in human reasoning: Causes and consequences: Lawrence Erlabum Associates, Inc.
[8] Nunnally, J. C. (1978). Psychometric theory: New York: McGraw Hill.
[9] Breward, M. (2007). Perceived privacy and perceived security and their effects on trust, risk, and user intentions. Paper presented at the Management of eBusiness, 2007. WCMeB 2007. Eight World Congress on the.
[10] Hinkin, T.R (1998). A brief tutorial on the development of measures for use in survey questionnaires. Organizational research methods, 1(1), 104-121
[11] McBride, M. (2004). Debiasing and trust enhancement techniques: Their influence in human acceptanceof automated decision-aided information. Doctoral Dissertation. Department of Industrial Engineering, North Carolina Agricultural & Technical State University, Greensboro, NC 27411.
[12] Chateauneuf, A. & Cohen, M. (1994). Risk seeking with diminishing margininal utility in a non-expected utility model. Journal of Risk and Uncertainty, 9, 77-91.
[13] Kim, K., Prabhakar, B., & Park, S. K. (2009). Trust, perceived risk, and trusting behavior in Internet banking. Asia Pacific J. Info. Sys, 19(3), 1-23.
[14] Harber, K.D. & Pennebaker, J.W. (1992). Overcoming traumatic conditions. In The Handbook of Emotion and Memory (S. A. Christiansen, Ed.), Hilldale, N.J: Erlbaum, 359-389.
[15] Bauer, R. A., & Cox, D. F. (1967). Risk taking and information handling in consumer behavior. Harvard Business School Press, Boston, MAd, 398.

.

BIOGRAPHIES

Emeka P. Idoye is currently a student at North Carolina A&T State University pursing his PhD in Industrial & Systems Engineering. His research interests have focused on cognitive human factors and manufacturing and service enterprise engineering.

Dr. Eui H. Park is a professor in the Department of Industrial and Systems Engineering at North Carolina A&T State University. He worked for Boeing Commercial Airplane Company as a senior engineer for four years from 1978, and returned to school for his doctorate with a Boeing Fellowship. Upon completion of his Ph.D., he joined North Carolina A&T State University and has since initiated and developed a successful interdisciplinary manufacturing program at the university as the Director of Manufacturing Initiatives. He is the founder of a teaching factory: Piedmont Triad Center for Advanced Manufacturing. Dr. Park was also the Chairperson of the Industrial and Systems Engineering Department for 16 years from July 1990. He has been an IIE (Institute of Industrial Engineers) Fellow since 2000. His fields of research are Human-Machine Systems Engineering and Quality Assurance.

Dr. Celestine A. Ntuen is a retired professor and the Director of the Institute for Human-Machine Studies at North Carolina A&T State University. He initiated a program in Human-Machine Systems Engineering at North Carolina A&T State University. He also started (and has since served as the program chair of) the Annual Symposium on Human Interaction with Complex Systems. He is interested in defining, modeling and designing frameworks for cognitive engineering as a discipline. He has published more than 100 papers in his field of interest.