The Status Quo and Effects of Undergraduate Students’ Cybersecurity Judgment: A study in China

Liu Chongrui 1, Wang Zhiqiang 2,3,4*, Wang Cong 5, Liu Yan 1, Wang Hongjie 1
1Department of Management, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
2Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
3State Information Center, Beijing, 100045, China
4Key Lab of Information Network Security, Ministry of Public Security, 200031, China
5Department of Economics and Management, Beijing City University, Beijing, 10083, China
*Corresponding author’s e-mail: wangzq@besti.edu.cn

Abstract. Internet users’ cybersecurity psychology and cognition play an important role in their cybersecurity behavior. Taking 347 Chinese undergraduate students for example, this study assessed internet users’ cybersecurity judgment and its effect on cybersecurity behavior in the Eastern countries. Results showed that the average percentage correct of cybersecurity judgment was 63.62%, cybersecurity judgment had positive impact on cybersecurity behavior. Furthermore, gender had a moderating effect on the relationship between cybersecurity judgment and cybersecurity behavior, compared with female, cybersecurity judgment had more positive influence on male’s cybersecurity behavior.

1. Introduction
Our life is becoming more and more dependent on cyberspace. However, guaranteeing security in cyberspace often proved to be difficult. The cybersecurity community has come to realize that the weakest link in a cybersecurity chain is human[1]. As the weakest link in the entire cybersecurity chain, internet users are increasingly being attacked by hackers[2]. Compared with cybersecurity professionals, internet users lack enough skill and knowledge about cybersecurity. As a specific group of internet users, undergraduate students are laxer about cybersecurity[3], whereas they receive far enough formal cybersecurity training[4]. Current research on undergraduate students’ cybersecurity psychology, cognition and behavior were conducted mainly in the Western countries[3, 4]. With the unique cultures in the Eastern countries, the research based on Chinese undergraduate students is helpful to deeply understand “the weakest link in cybersecurity” in global context. Furthermore, it is concluded that psychological factor such as internet users’ perceived threat susceptibility, self-efficacy has an important effect on cybersecurity behaviour[5]. However, the process starting with psychology and ending with behavior involves an important mediating factor of cognitive judgment, which is the strongest predictor of behaviour[6], little research focuses on how internet users’ cognitive judgments on cybersecurity risk influence their behaviour[4].
To fill these gaps, this study aimed to explore the status quo of Chinese undergraduate students’ cybersecurity judgment, furthermore examine the effect of cybersecurity judgment on cybersecurity behavior. This study conducted in the Eastern country would contribute to enrich current research in a global context. In addition, the study empirically verified the effect of cybersecurity judgment on cybersecurity behavior, as well as the gender difference among it, which echoed Anwar et al.’s calling[7] researchers to investigate the gender differences in cybersecurity behavior.

2. Research hypotheses

2.1 Cybersecurity Judgment and Cybersecurity Behavior

The protection motivation theory argues that internet users confronted with a threat will evoke two mediating cognitive process: threat appraisal and coping appraisal[8]. Threat appraisal evaluates the seriousness of the threat (perceived severity) and likelihood of suffering from it (perceived vulnerability). Coping appraisal assess the effectiveness of the possible responses to the threat (response efficacy) and personal ability to effectively perform the desired response (self-efficacy). The two appraisal processes determine whether individuals will respond with a maladaptive coping response to take actions. In line with the protection motivation theory, it is concluded that internet users confronted with cybersecurity incidents would make cognitive judgment about the risk in cybersecurity incidents (threat appraisals), under the condition that it is easy to cope with and avert the threatened danger (coping appraisal). The higher the correct rate of cognitive judgment is, the more likely he takes some protective action, such as preventive behavior. Hence, it can be inferred that the stronger internet users’ ability to make correct judgments on cybersecurity incidents are, the more likely they take cybersecurity behavior. Therefore, we hypothesize:

Hypothesis 1: The correct rate of cybersecurity judgment has a positive effect on cybersecurity behavior.

2.2 The Moderating Role of Gender

There are significant gender difference in individuals’ cybersecurity perception, attitude and behavior, for example, Male and female have different views on risk[9], Hajli & Lin[10] proved this insight in their conclusion that female are more concerned about privacy risks and perceived control when sharing information on social networks. Ifinedo[11] and Anwar et al.[7] explored the gender difference in employees’ cybersecurity behaviors, which reached the conclusion that male’s cybersecurity behavior was higher than that of female. It can be inferred that, although the female are more sensitive to cybersecurity risk, the male are more likely to take actions to remove the risk. Hence, under the same capability in cybersecurity judgment, male are more likely to take cybersecurity behavior than female. Therefore, we propose:

Hypothesis 2: Gender has a moderating effect on the relationship between cybersecurity judgment and cybersecurity behavior. Specifically, compared with female, the cybersecurity judgments have a stronger positive impact on male’ cybersecurity behavior.

3. Methodology

3.1 Sample and Procedure

We sent out an online survey to undergraduate students in China. As a result, 361 undergraduate students completed the survey. Among all the questionnaires, some samples were excluded because of the missing answers. In total, 347 undergraduate students were included in our study. There was sufficient variation in terms of gender (44.38% male); 10.95% were freshmen, 37.46% sophomores, 12.68% juniors, and 38.90% seniors; undergraduate students’ internet age ranges from less than 2 years (16.43%), 2-5 years (17.87%), 5-10 years (36.89%), to more than 10 years (28.82%). To maximize the anonymity of participants, other demographic characteristics such as ethnicity were not collected in this study.
3.2 Measures

Cybersecurity Judgment. This study applied Yan’s cybersecurity judgment questionnaire[4] to assess how well Chinese undergraduate students judge cybersecurity risks. This scenario-based questionnaire is composed of 16 real-life scenarios about cybersecurity, one scenario is: “Li Hong is an officer of the federal government who has access to confidential information. Her secretary’s computer stopped working but there is urgent and important work to do. Her secretary asks Li Hong if she can use Li Hong’s computer, Li Hong does not agree”.

The scale uses a 6-point Likert scale, with 1= lowest risk, 6= highest risk. Among the 16 scenarios, one-half concern risky cybersecurity actions (e.g., clicking the link to purchase a virus scanner) and the other half concern safe cybersecurity actions (e.g., deciding not to click the link to purchase a virus scanner). For the safe cybersecurity actions, participants’ responses were reversely coded prior to data analysis.

In order to obtain the percentage correct of cybersecurity judgment for each sample, each respondent’s Likert 6 point score was further collapsed into a dichotomous score (0=incorrect, 1=correct), and the dichotomy was widely used in empirical research. Specifically, if the respondent’s judgment is 1, 2 or 3 for a risky scenario (the risk coefficient is low), then the respondent’s judgment is incorrect and thus coded as 0; if the respondent’s judgment is 4, 5 or 6 (the risk coefficient is high), then the respondent’s judgment is correct and thus coded as 1. According to this, the percentage correct of each respondent is determined by the number of correct judgments. Similarly, a percentage correct of each scenario was obtained by averaging correct judgments of all participants on a scenario.

Cybersecurity behavior. Cybersecurity behavior is measured by Claar & Johnson’s computer security usage scale[12], which contains five items that measure the extent to which respondents take preventative behavior against cybersecurity risks. This scale uses the Likert 5 point scale, with 1 = never, 5 = always, the Cronbach ’s alpha is 0.70.

4. Results

4.1 The Situation of Chinese Undergraduate Students’ Cybersecurity Judgment

4.1.1 The Overall Percentage Correct of Cybersecurity Judgment

For the 347 students in the study, their overall percentage correct of cybersecurity judgment on the 16 scenarios under the two conditions was 63.62% (SD = 15.59%). That is, they got about 10 out of 16 scenarios correct on average. Since making cybersecurity judgment correct or incorrect on the 16 scenarios follows a typical binomial distribution with 16 as independent trials and 0.50 as the chance of making the correct judgment in each trial. On the basis of Yan et al.[4], the percentage of respondents’ random guessing is defined a probability of 0.50 being correct, this study set 0.50 as the low baseline for cybersecurity judgment. While the percentage of respondents’ consistent correctness is defined a probability of 0.90 being correct, this study sets 0.90 as the high benchmark of cybersecurity judgment.

This study chooses the significance level of 0.10 (that is, a probability of 0.90 being correct). The one-sample T-test showed that, using the benchmark of 50% percentage correct, the average percentage correct of the sample (65.41%) was significantly higher than 50%, t(347) = 16.27, p <0.001, indicating that these students as a group were able to make sensitive judgments rather than relying on random guessing. In contrast, using the benchmark of 90% percentage correct, the average percentage correct of the sample is significantly lower than 90%, t (347) = 31.52, p < 0.001, indicating that these students failed consistently achieving correctness in making judgments.

4.1.2 The Percentage Correct of Cybersecurity Judgment among the 347 Participants.

Some significant differences exist across individual students. Specifically, the percentage correct of 112 students (32.28%) is less than 50%, the percentage correct of 217 students (62.54%) is between 56% and 90%; 18 students (5.19%) are higher than 90%. 112 students (approximately one-quarter) with a
percentage correct of less than 50% can be considered the weakest link and should be given special cybersecurity precautions and interventions.

4.1.3 The Percentage Correct of Cybersecurity Judgment across the 16 Scenarios.
As shown in Figure 1, across the 16 scenarios, the percentage correct of 7 scenarios (o1s, p2s, o3s, o5s, p5s, p6s, o7s) is less than 50%, 4 scenarios (p1s, p3s, o4s, o8s) have the correct rate between 50% - 90%, 5 scenarios (o2s, p4s, o6s, p7s, p8s) have the correct rate above 90%. This indicates that undergraduate students’ percentage correct across the 16 scenarios vary in a certain degree, while scenarios o1s, p2s, o3s, o5s, p5s, p6s, o7s were the most difficult for students to answer correctly and thus can be considered the weakest link in judging different aspects of cybersecurity actions. Specifically, the scenario with the lowest percentage correct is about E-mail linking, which indicates that undergraduate students are more sensitive to potential cybersecurity intrusions.

4.2 Correlation Analysis
As is shown in table 1, the correlation between the percentage correct of cybersecurity judgment and gender ($\beta = 0.20, p < 0.01$), internet age ($\beta = 0.41, p < 0.01$), cybersecurity behavior ($\beta = 0.31, p < 0.01$) was significant, the correlation between cybersecurity behavior and internet age was significant ($\beta = 0.28, p < 0.01$).

|       | M  | S  | D  | 1  | 2  | 3  | 4  | 5  | 6  |
|-------|----|----|----|----|----|----|----|----|----|
| 1.gender | 1.56 | 0.50 | 1 | | | | | | |
| 2.age | 20.65 | 1.61 | 0.08 | 1 | | | | | |
| 3.internet age | 2.78 | 1.04 | 0.16* | 0.12* | 1 | | | | |
| 4.grade | 2.88 | 1.23 | 0.03 | 0.62** | 0.10 | 1 | | | |
| 5.cyberspace behavior | 3.26 | 0.74 | -0.02 | -0.04 | 0.28** | 0.03 | 1 | | |
| 6.cyberspace judgment | 0.64 | 0.16 | 0.20** | -0.02 | 0.41** | -0.05 | 0.31** | 1 | |

4.3 Test of Hypotheses
We conducted hierarchical regression analyses to test hypothesis (Table 2). Hypothesis 1 predicted that the percentage correct of cybersecurity judgment has positive effect on cybersecurity behavior. As illustrated in model 2, the percentage correct of cybersecurity judgment was significantly positively
related to cybersecurity behavior ($\beta = 0.24, p < 0.001$), H1 was supported. Hypothesis 2 predicted that gender moderate the positive effect of percentage correct of cybersecurity judgment on cybersecurity behavior. The result in model 3 suggested that the interaction of gender and percentage correct of cybersecurity judgment was significantly negatively related to cybersecurity behavior ($\beta = -0.15, p < 0.01$), H2 was supported.

Table 2. Results of hierarchical regression analysis

|                  | Model1 | Model2 | Model3 |
|------------------|--------|--------|--------|
| Step1: control variable |        |        |        |
| Grade            | 0.09   | 0.09   | 0.10   |
| age              | -0.11  | -0.10  | -0.10  |
| Internet age     | 0.25***| 0.18** | 0.16** |
| Step2: main effect |        |        |        |
| gender           | -0.12* | -0.13* |        |
| Cybersecurity judgment | 0.24***| 0.28***|        |
| Step3: moderating effect |        |        |        |
| gender*          |        |        | -0.15**|
| Cybersecurity judgment |        |        |        |
| $R^2$ change     | 0.10   | 0.05***| 0.02** |
| F change         | 9.17***| 10.27***| 8.20** |

5. Discussion

This study quantitatively examines “human is the weakest link phenomenon” from the cybersecurity judgment perspective in Chinese context. Overall, the findings demonstrated that the average percentage correct of cybersecurity judgment was about 63.62%. Specifically, significant variations in the percentage correct has also been found among the 347 Chinese undergraduate students, across the 16 scenarios, and between the intuitive and rational conditions. Furthermore, this study found that the percentage correct of cybersecurity judgment has significantly positive effect on cybersecurity behavior. Meanwhile, gender plays a moderating role in the relationship between the percentage correct of cybersecurity judgment and cybersecurity behavior. Compared with female, cybersecurity judgments has stronger predictive effect on male’s cybersecurity behavior. This is the first benchmark assessment of this kind in Eastern context. In cybersecurity behavioral research, most conclusions were reached in the Western background. As Yan et al.[4] calling for understanding the cybersecurity judgement in different samples, this study discuss the different understanding of cybersecurity judgment and behavior of people with different cultural values. Furthermore, this research proved empirically that cybersecurity judgment has significant effect on cybersecurity behavior, and furthermore, gender has a significant moderating role in the relationship between cybersecurity judgment and cybersecurity behavior. Specifically, male were more inclined to take cybersecurity behavior, which contributes to the existing literature by discovering and explaining gender differences in the context of cybersecurity cognitive judgment and behavior.
6. Conclusion

It has been widely recognized that internet users rather than technology systems are the weakest link in cybersecurity. However, research on psychology of cybersecurity has failed to examine the weakest link phenomenon. Taking Chinese undergraduate students as example, this present study investigated the state quos of ordinary internet users’ cybersecurity judgment. In addition, this study found that cybersecurity judgment was a predictive variable of cybersecurity behavior, and the predictive effect had significant gender difference.

Acknowledgments

This research was financially supported by the National Key Research and Development Plan (2018YFB1004101), China Postdoctoral Science Foundation Funded Project (2019M650606), Key Lab of Information Network Security, Ministry of Public Security (C19614), Special fund on education and teaching reform of Besti (jy201805), the Fundamental Research Funds for the Central Universities(328201910), key laboratory of network assessment technology of Institute of Information Engineering, Chinese Academy of Sciences.

References

[1] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & security, 32, 90-101.
[2] D’Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the "Dark Side" of Information Technology Use. Communications of the Association for Information Systems, 35(5), 109-118.
[3] Schaik, P. V., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behavior . Computers in Human Behavior, 75.
[4] Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., & Chen, Q., et al. (2018). Finding the weakest links in the weakest link: how well do undergraduate students make cybersecurity judgment?. Computers in Human Behavior, 84.
[5] Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems, 92, 25-35.
[6] Roghanizad, M. M., & Neufeld, D. J. (2015). Intuition, risk, and the formation of online trust. Computers in Human Behavior, 50, 489-498.
[7] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees’ cybersecurity behaviors. Computers in Human Behavior, 69(C), 437-443.
[8] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.), Social psychophysiology. New York: Guilford Press.
[9] Gustafson, P. E. (1998). Gender differences in risk perception: Theoretical and methodological perspectives. Risk Analysis, 18, 805-811.
[10] Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), 111-123.
[11] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effect of socialisation, influence, and cognition. Information & Management, 51(1), 69-79.
[12] Claar, C. L., & Johnson, J. (2012). Analyzing home pc security adoption behavior.Journal of Computer Information Systems, 52(4), 20-29.