Postprint of a Risk Evaluation System for Consumer Personal Privacy Information Disclosure in Mobile Commerce

Authors: mutual roof ridges, Wang Xiwei, Jia Ruonan, Wang Lei

Date: 2023-08-27T00:00:00+00:00

Abstract

[Purpose/Significance] The risk assessment of personal privacy information disclosure by mobile commerce consumers plays a crucial role in understanding consumer privacy disclosure behavior and enhancing the protection of consumer privacy information security by platforms and merchants. [Methods/Process] By integrating the characteristics of mobile commerce, and based on a review of relevant literature and questionnaire surveys, this study constructs a risk indicator system for personal privacy information disclosure by mobile commerce consumers, employs the fuzzy comprehensive evaluation method to determine indicator weights, and conducts empirical analysis using the Taobao APP. [Results/Conclusion] The results indicate that consumer self-vulnerability risk carries the highest risk level among all indicators, while mobile terminal vulnerability risk has the lowest weight score. Furthermore, weak consumer security awareness accounts for the largest weight, suggesting that enhancing consumers' own privacy security awareness is the most critical aspect of protecting consumer privacy information security.

Full Text

Abstract

[**Purpose/Significance**] The risk assessment of consumer privacy information disclosure in mobile commerce plays a crucial role in understanding consumer privacy disclosure behaviors and enhancing the protection of consumer privacy information security by platforms and merchants. [**Method/Process**] Combining the characteristics of mobile commerce, this study constructs a risk evaluation index system for consumer privacy information disclosure in mobile commerce based on a review of relevant literature and questionnaire surveys. The fuzzy comprehensive evaluation method is employed to determine the weights of

evaluation indicators, and an empirical analysis is conducted using Taobao APP as a case study. [**Result/Conclusion**] The data results indicate that consumer vulnerability risk poses the greatest relative risk compared to other indicators, while mobile terminal vulnerability risk receives the lowest weight score. Additionally, weak consumer security awareness carries the highest weight, demonstrating that improving consumers'privacy security awareness is the most critical aspect of protecting consumer privacy information security.

Keywords: mobile commerce; personal privacy; information disclosure; risk assessment

1 Introduction

As mobile commerce increasingly influences public life, people are using mobile apps for shopping, mobile payments, utility bill payments, and other applications more frequently. While consumers enjoy diversified and personalized services provided by enterprises in mobile commerce, they also face severe personal privacy information security issues. The provision and use of these convenient mobile services are based on the collection and analysis of consumer privacy information; to enjoy more accurate personalized services, consumers must disclose more privacy information to merchants. During the processes of acquisition, use, transmission, and storage by merchants, consumer privacy information often faces risks of leakage, misuse, and theft. In October 2017, the Pizza Hut website was hacked, resulting in the leakage of personal privacy information of over 60,000 users who placed orders through the website and mobile app. This information included important personal privacy data such as names, billing addresses, postal codes, delivery addresses, email addresses, payment card numbers, expiration dates, and credit card verification codes. The security risks of consumer privacy information in mobile commerce have attracted increasing attention from both academia and industry.

Scholars both domestically and internationally have conducted research on privacy information risks from various perspectives, including privacy risk perception, privacy risk attitudes, and privacy information risk management and assessment. Regarding privacy information risk assessment, foreign scholars such as W. Tianshui et al. proposed a new information system security and privacy risk assessment model based on network analysis and grey system theory, referencing the GB/T20984-2007 ISRAs standard. J. Friginal et al. studied risk assessment methodologies for privacy risks that users may encounter when using location-based services. R. Jiang et al. proposed a wireless network privacy risk assessment method based on attack trees, using attack tree models to determine potential attack sequences that attackers might launch against privacy protection systems in wireless networks, thereby guiding decision-makers to adopt appropriate location privacy protection measures. Domestic scholar Wang Kan analyzed and classified risk factors and causes in mobile commerce transactions, constructing a risk evaluation index system through empirical research. Zhang Qiujin studied privacy security risks and risk assessment models

in cloud computing services. Kuang Qingqing used association analysis and game theory methods to analyze the sources of risk events for user privacy information generated during internet usage and constructed a risk assessment index system. Zhu Guang et al. qualitatively analyzed privacy risk factors in social networks under big data environments and empirically analyzed privacy risks on social network platforms. Zhu Yijie studied privacy leakage risk assessment in location-based services, designing two location privacy leakage risk assessment schemes and conducting simulation experiments.

Existing research shows that foreign scholars tend to focus on privacy security attacks that users suffer during information system usage, while domestic scholars emphasize exploring the influencing factors that cause user privacy security issues. Overall, current research both domestically and internationally primarily concentrates on privacy information risks in information systems and social networks, with relatively few studies specifically addressing risk evaluation of consumer privacy information disclosure in mobile commerce.

2 Evaluation Index Selection

This study attempts to answer three key questions: (1) What are the risk indicators for consumer privacy information disclosure in mobile commerce? (2) What evaluation methods should be used for consumer privacy information disclosure in mobile commerce? (3) How can the constructed evaluation indicators and methods be applied through typical cases? Based on a review of relevant literature and combining the characteristics of mobile commerce consumer behavior, this study constructs risk evaluation indicators for consumer privacy information disclosure in mobile commerce.

2.1 Preliminary Selection of Evaluation Indicators

(1) Basis for indicator construction. Through a systematic review and analysis of existing literature on privacy information risk evaluation, representative research outcomes were identified and summarized in Table 1 , serving as a foundation for constructing the evaluation index system in this study.

As shown in Table 1, risks to consumer privacy information in mobile e-commerce include both traditional information system security risks (such as platform vulnerability risks and external environmental threat risks) and risks unique to mobile e-commerce services (such as location-based service risks in mobile networks, user behavior risks, and risks caused by third-party actions). In the mobile e-commerce environment, analyzing and assessing these risks is a prerequisite for effectively protecting consumer privacy information. Based on previous research and referencing the BS7799 (ISO/IEC17799) information security assessment standard and information system security models, this study selected 19 risk evaluation indicators for consumer privacy information disclosure in mobile e-commerce. These indicators were categorized into four dimensions: mobile terminal vulnerability risk, mobile network environment

risk, consumer vulnerability risk, and external threat risk. The indicators and their explanations primarily reference the sources shown in Table 2 .

(2) Indicator refinement. After preliminary selection of the evaluation indicators, the Delphi method was employed to assess the rationality and completeness of the indicators. Five industry and academic experts in mobile commerce were selected, and two rounds of opinion solicitation were conducted. Based on the experts' suggestions, the following revisions were made: First, the indicator "mobile terminal or device loss" under the "mobile terminal vulnerability risk" dimension was removed, as it was considered an individual consumer behavior without universal risk characteristics, and mobile terminals serve as carriers for mobile commerce platform apps, lacking correlation with other indicators in this dimension. Second, the names of two indicators were standardized: "location-based service risk" under the "mobile network environment risk" dimension was refined to "location service risk," and "privacy information sharing risk" under the "consumer vulnerability risk" dimension was modified to "privacy association setting" to eliminate ambiguity.

2.2 Questionnaire Design and Pre-test Distribution

(1) Questionnaire design. The survey questionnaire for evaluating consumer privacy information disclosure risk in mobile commerce consisted of two parts: The first part collected basic demographic information (age, gender, education, occupation, etc.) and mobile commerce application usage patterns (duration and frequency of use). The second part measured consumer privacy information disclosure risk in mobile commerce, using statements to express the feasibility and rationality of each evaluation indicator. Each statement was expressed in accessible language to facilitate questionnaire completion.

(2) Questionnaire and scale adjustment. Before formal distribution, a small-scale test was conducted with 100 undergraduate students, yielding 87 valid responses. The 19 items were coded according to the four dimensions, as shown in Table 3 .

(3) Pre-test reliability analysis. Using Cronbach' s coefficient to measure questionnaire reliability, the overall Cronbach' s alpha for the 19 items was 0.906, indicating high reliability. Among the four dimensions, mobile network environment risk, consumer vulnerability risk, and external threat risk achieved overall reliability scores of 0.871, 0.807, and 0.857, respectively (all above 0.80), while mobile terminal vulnerability risk scored 0.797, approaching 0.80. These results demonstrate that all four risk analysis dimensions meet the required standards.

(4) Pre-test validity analysis. Before conducting exploratory factor analysis (EFA), KMO and Bartlett' s sphericity tests were performed using SPSS 19.0. The results showed KMO = 0.836 and Bartlett's significance < 0.001, indicating that the pre-test sample met overall validity requirements for factor analysis. Using principal component analysis with varimax rotation, four common factors

were extracted, explaining 66.259% of the variance in 19 variables (exceeding 60%). The rotation converged after six iterations. After processing the rotated component matrix (sorted by size, suppressing small coefficients with absolute value < 0.4), CVR1 was found to cross-load on the MTVR dimension and was deleted, while MTVR5 showed similar loadings on two dimensions and was also deleted. The revised risk evaluation indicators are presented in Table 4 .

2.3 Formal Survey

(1) Questionnaire distribution. The formal survey employed both online and on-site distribution methods. Online distribution was conducted through the "Wenjuanxing" platform, while on-site distribution occurred in university classrooms. Before distribution, the questionnaire content and completion instructions were explained to ensure quality. A total of 300 questionnaires were collected, with 252 valid responses.

(2) Exploratory factor analysis. The same analytical method as the pre-test was applied using SPSS 19.0. The results showed KMO = 0.843 and Bartlett' s significance < 0.001. Four common factors were extracted, explaining 66.579% of variance in 17 variables, with rotation converging after five iterations. The factor structure aligned with the proposed dimensions.

(3) Confirmatory factor analysis. Using AMOS 21.0, confirmatory factor analysis (CFA) was conducted on the second sample (n = 126). The model included 17 observed variables and 4 latent variables, with maximum likelihood estimation. The standardized loading coefficients are shown in Figure 1 [Figure 1: see original paper], and the estimated relationships between observed and latent variables are presented in Table 5 .

According to conventional criteria, when the absolute C.R. value exceeds 2.58, parameter estimates reach the 0.01 significance level, and when p < 0.001 (marked as "*** "), the model achieves significant levels. Table 5 shows satisfactory model significance. AMOS model fit indices confirmed that the evaluation index system meets test requirements.

3 Construction of the Evaluation Index System

3.1 Establishing the Hierarchical Model

A hierarchical model was established for evaluating consumer personal privacy information disclosure risk, comprising three levels: target layer, criterion layer, and index layer. The target layer assesses the risk level of consumer privacy information disclosure. The criterion layer includes four dimensional indicators: mobile terminal vulnerability risk, mobile network environment risk, consumer vulnerability risk, and external threat risk. The index layer contains 17 specific indicators. The hierarchical model is illustrated in Figure 2 [Figure 2: see original paper].

3.2 Constructing Pairwise Comparison Judgment Matrices

Through expert consultation, pairwise comparison judgment matrices were constructed. Five experts were selected: two in user privacy research, two in mobile e-commerce research, and one mobile e-commerce user (numbered 1-5). Experts scored the relative importance of indicators based on their experience, using Saaty' s 1-9 scale to construct judgment matrices for both criterion and index layers.

3.3 Indicator Weight Calculation and Consistency Test

Given the complexity and diversity of mobile commerce consumer privacy disclosure risk indicators and varying expert judgments, consistency test was performed to avoid subjective bias. The consistency index (CI) was calculated, yielding CI = 0.0347 and CR = 0.0390 (< 0.1), indicating satisfactory consistency. The normalized weight vector was calculated using the geometric mean method, resulting in M = [0.0549, 0.2619, 0.5659, 0.1173]. Weights for each matrix were calculated and averaged to obtain relative weights, which were then synthesized to calculate overall weights relative to the system target, as shown in Table 6 .

3.4 Evaluation Process

Based on fuzzy comprehensive evaluation (FCE), the evaluation process involves: (1) establishing the factor set of consumer privacy information disclosure risk indicators; (2) determining the evaluation grade set, categorized into five levels: {very low, low, medium, high, very high}; (3) constructing the membership matrix through user perception scoring; and (4) calculating comprehensive evaluation results using either the maximum membership principle or weighted average principle to determine the final risk level. The quantitative values for evaluation elements are shown in Table 7 .

4 Empirical Analysis

4.1 Sample Selection

Taobao APP, launched by Alibaba Group, is a mobile shopping application that facilitates consumer purchases via smartphones and tablets in mobile network environments. According to iResearch' s 2017 China Mobile E-commerce Industry Report, Taobao' s monthly independent mobile device coverage far exceeds other e-commerce platforms. This study selects Taobao APP as the research object for empirical analysis using the constructed risk evaluation indicators.

Since most indicators are qualitative and difficult to measure objectively, data were collected through expert and user scoring, with fuzzy mathematics membership methods used for quantification. Five network information security experts and three APP developers evaluated "mobile terminal vulnerability

risk" and "mobile network environment risk," while eight Taobao APP users assessed "consumer vulnerability risk" and "external threat risk." The demographic information of these 16 evaluators is shown in Table 8 .

4.2 Risk Evaluation Process

First, expert scores were converted into a membership matrix. For each indicator, single-factor evaluation was conducted by converting the proportion of experts assigning each risk level into membership vectors. For example, for "APP vulnerability risk (b11)," 12.5% of experts rated it as "very low," 37.5% as "low," 37.5% as "medium," 12.5% as "high," and 0% as "very high," yielding the membership vector r11 = (0, 0.125, 0.375, 0.375, 0.125). This process generated the membership matrix Ri for each indicator category Bi.

Second, comprehensive evaluation was performed by multiplying the weight vector W' i with the membership matrix Ri using the product-sum operator to obtain the comprehensive evaluation result Ci for each dimension. The fuzzy evaluation matrix CB was formed by combining results from all four dimensions.

Third, the final evaluation result C was calculated by multiplying the dimension weight vector W' with matrix CB: C = (0.0146, 0.1114, 0.1529, 0.1274, 0.0017). Since the membership degrees showed minimal differences, the weighted average principle was applied to determine the risk level. Using the formula M = (Σ Mv $\cdot$ cv)/Σ cv, the calculated value C = 49.4036 falls within (40,60], indicating that the risk level of consumer privacy information disclosure on Taobao APP is "medium."

4.3 Discussion of Evaluation Results

(1) Analysis of first-level indicators. Among the primary indicators, consumer vulnerability risk (B3 = 0.5527) carries the highest weight, indicating it poses the greatest risk to consumer privacy information security in mobile commerce. This suggests consumers must strengthen privacy protection awareness and risk response capabilities. Weak security awareness, neglect of privacy policies, simple passwords, and using payment accounts to log into multiple shopping sites all pose significant threats. Education on privacy security risks should be enhanced, improving network literacy and privacy protection awareness while avoiding excessive disclosure of personal information.

Mobile network environment risk (B2 = 0.2914) and external threat risk (B4 = 0.1026) also significantly impact consumer privacy information security. Risks include data sharing between platforms, location-based services collecting trajectory information, and inadequate privacy legislation. Mobile terminal vulnerability risk (B1 = 0.0533) has the lowest weight, indicating that mobile commerce platforms pose relatively low risk from technical investment, institutional safeguards, and user security experience perspectives.

(2) Analysis of second-level indicators. Among all secondary indicators,

weak consumer security awareness (B31 = 0.6011) carries the highest weight, confirming that improving consumer privacy awareness is paramount. APP vulnerability risk (B11 = 0.5691) ranks second, highlighting the importance of application security. Illegal privacy information trading (B42 = 0.5550) ranks third, indicating an urgent management issue requiring government attention. Network communication protocol vulnerability (B21 = 0.0333) has the lowest weight, suggesting that attacks exploiting protocol vulnerabilities pose minimal threat to consumer privacy security due to improved network security technologies.

The government should strengthen the external environment for consumer privacy protection by enacting specialized laws, improving existing regulations, accelerating network integrity system construction, and enhancing supervision to precisely target various privacy risks.

5 Research Conclusions

At the theoretical level, this study combines the GB/T20984-2007 information security assessment standard with mobile e-commerce consumer behavior characteristics. Through literature review and Delphi and questionnaire methods, it constructs a four-dimensional evaluation index system covering mobile terminal vulnerability risk, mobile network environment risk, consumer vulnerability risk, and external threat risk. The fuzzy comprehensive evaluation method was used to determine indicator weights.

At the practical level, empirical analysis of Taobao APP using eight experts and eight users demonstrates that consumer vulnerability risk poses the greatest threat, while mobile terminal vulnerability risk poses the least. Among secondary indicators, weak consumer security awareness carries the highest weight, while network communication protocol vulnerability carries the lowest. The study proposes management strategies from three perspectives: enhancing consumer privacy awareness education, strengthening information security protection by platforms and APP developers, and improving the external legal and regulatory environment.

Limitations include the subjective nature of expert and user scoring, which may introduce bias, and the narrow scope focusing only on Taobao APP. Future research should employ quantitative analysis methods and expand the sample range to enhance the universality of the evaluation indicators.

References

[1] Pizza Hut hacked: How to protect personal data security for 60,000 users? [EB/OL]. [2017-10-20]. http://sh.qihoo.com/pc/detail?check=30f997d3de1f6669&sign=360_{e39369d1}&url=
10-20/15828374. [2] WANG T, DUONG T D, CHEN C C. Intention to disclose personal information via mobile applications: a privacy calculus perspective [J]. International journal of information management, 2016, 36(4): 531-542.

[3] HAJLI N, LIN X. Exploring the security of information sharing on social networking sites: the role of perceived control of information [J]. Journal of business ethics, 2016, 133(1): 111-123. [4] XIAO Haiqing. Analysis of factors influencing user privacy risk perception in e-commerce personalized recommendation adoption [D]. Wuhan: Central China Normal University, 2015. [5] FOGEL J, NEHMAD E. Internet social network communities: risk taking, trust, and privacy concerns [J]. Computers in human behavior, 2009, 25(1): 153-160. [6] MATT C, PECKELSEN S P. Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior [C]// System Sciences (HICSS), USA: 2016 49th Hawaii international conference on. Washington: IEEE Computer Society, 2016: 4832-4841. [7] ZHU Guang, CUI Weijun, ZHANG Weiwei. Research on big data privacy risk management framework from the perspective of information lifecycle [J]. Information and documentation services, 2016, 36(1): 99-105. [8] DI Liya. Research on privacy leakage impact assessment in big data environment [J]. Journal of intelligence, 2016(4): 141-146. [9] WU T, GANG Z. A new security and privacy risk assessment model for information system considering influence relation of risk elements [C]// Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference on. Washington: IEEE Computer Society, 2014: 233-238. [10] FRIGINAL J, GUIOCHET J, KILLI J I A M O. Towards a privacy risk assessment methodology for location-based systems [C]// International conference on mobile and ubiquitous systems: computing, networking, and services. Japan: Springer, Cham, 2013: 748-759. [11] JIANG R, LUO J, WANG X. An attack tree based risk assessment for location privacy in wireless sensor networks [C]// Wireless communications, networking and mobile computing (WiCOM), China: 2012 8th International Conference on. Washington: IEEE Computer Society, 2012: 1-4. [12] WANG Kan. Research on mobile commerce transaction risk assessment and control decision based on evidence theory [D]. Wuhan: Huazhong University of Science and Technology, 2009. [13] ZHANG Qiujin. Research on cloud computing privacy security risk assessment [D]. Kunming: Yunnan University, 2015. [14] KUANG Qingqing. Risk assessment based on personal privacy leakage [D]. Guiyang: Guizhou University, 2016. [15] ZHU Guang, FENG Minging, CHEN Ye, et al. Research on fuzzy evaluation of social network privacy risk in big data environment [J]. Information science, 2016, 34(9): 94-98. [16] ZHU Yijie. Analysis and evaluation of privacy leakage risk in location-based services [D]. Guiyang: Guizhou University, 2016. [17] CHEN Min, HU Zuojin, CAI Shuzhen. Research on information system security risk assessment model [J]. Computer applications and software, 2007, 24(6): 73-77. [18] China Internet Data Consulting Center. 2013 Mobile Privacy Security Evaluation Report [EB/OL]. [2017-12-13]. http://www.199it.com/archives/99542.html. [19] ZHANG Cheng. Research on mobile internet privacy leakage [D]. Beijing: Beijing University of Posts and Telecommunications, 2012. [20] QIU Junping, LI Yanhong. Exploration of user privacy security issues in social networks [J]. Information and documentation services, 2012, 33(6): 34-38. [21] CHEN Yunhai, HUANG Lanqiu. Research on the impact of big data processing on e-commerce [J]. Telecommunications

science, 2017, 29(3): 17-21. [22] ISO/IEC17799. Information technology—Code of practice for information security management [EB/OL]. [2017-11-20]. http://bastille-linux.sourceforge.net/jay/iso.pdf. [23] WU Y, FENG G, WANG N, et al. Game of information security investment: impact of attack types and network vulnerability [J]. Expert systems with applications, 2015, 42(15/16): 6132-6146. [24] WU Minglong. Structural equation model: AMOS operation and application [M]. Chongqing: Chongqing University Press, 2009. [25] iResearch. 2017 China Mobile E-commerce Industry Research Report [EB/OL]. [2017-02-20]. http://www.askci.com/news/hlw/20170313/10453493170.html. [26] WANG Xiwei, LI Jiaxing, YANG Mengqing, et al. Research on the influence of mobile social software privacy security on usage intention [J]. Library and information service, 2016, 60(15): 21-27.

Author Contributions

Xiang Mengmeng: Responsible for paper writing, revision, data collection, and data processing.
Wang Xiwei: Responsible for research proposition, research framework design, paper writing, and final revision.
Jia Ruonan: Responsible for data processing and abstract translation.
Wang Lei: Responsible for literature collection and proofreading.

Note: Figure translations are in progress. See original paper for figures.