Are iPhone users more secure when using mobile enterprise systems?*

The difference of the perceived security of Enterprise Systems between IOS and Android users

Yang Wu

15 April 2021

Abstract

Organizations are adopting mobile technologies for various business applications including Enterprise system (ES) to increase the flexibility and to gain sustainable competitive advantage. At the same time, end-users are exposed to security issues when using mobile technologies. Users' usage habits and users' attitudes towards those potential security issues would have a significant impact to the perceived security of ES. Here comes the question: will iPhone users have higher perceived security than Android users? Through the propensity score matching and regression model, we have the answer.

Keywords: Security Issues; Perceived security measurement; iPhone & Android; Matching

Contents

*Code and data are available at: https://github.com/yangg1224/Security-of-Enterprise-System.git.

1 Introduction

Mobile Enterprise System (ES) has more unique advantages than traditional enterprise systems. With a mobile enterprise platform, the entire company can be moved to the internet. Therefore, users who have permission can remotely access the enterprise database with any device equipped with a browser. Easy and convenient accessibility of data from mobile devices anywhere and anytime has made a significant change in people's working style (Al Bar et al. 2011). People are no longer confined to working in the office, and any place can be their workstation. Besides, increasing business applications take advantage of mobile devices features such as a touchscreen, camera, video, voice, and other advanced functions to maximize the productivity. (Rodrigues, Ruivo, and Oliveira 2021).

These advantages have created a vulnerability. The primary design purpose for the mobile device is its portability, not its security, which gives mobile enterprise systems weaker defense capabilities (He, 2013). There are many challenges and issues stemming from a lack of users' awareness and negative attitudes. It is increasingly hard for an enterprise to maintain resource safety since the interaction between the user and device boost sharply. The features of these interactions are often unplanned and lack of supervision, which makes the leakages of the enterprise information possible(Matkerimov and Yakovlev 2020).

The dependent variable in my project is the perceived security of mobile ES. Many researchers have widely discussed the definition of mobile ERP system security. Although their understanding of the ERP security is strongly based on their specific domains, some aspects of the understanding of mobile ERP security are shared. (Siponen and Oinas-Kukkonen 2007) define security as the protection of resources to attain the objectives of integrity, availability, and confidentiality. With regards to "integrity", the authors suggest the metadata cannot be modified without authorization, while "availability" means that authorized person can access information anytime and anywhere. Finally, "confidentiality" refers to certain actions being implemented to prevent information leakage.

As we all know, compared with Android devices, iPhone has relatively closed platform, which gives it higher security performance. But users' usage habits also have a huge impact towards the perceived security. For example, if users tend to use public Wi-Fi at coffee shop, the perceived security of ES would be lower. Because the system has more risk of information leakage. (whether they update operating system; how they deal with pop up security warning . . .) All those uncertainties raise my interest to figure it out.

The purpose of this project is to examine whether iPhone users (IOS) are securer than Android users when using mobile ES. The intervention is using iPhone as mobile device. The questionnaire survey is the chosen method for collecting data from mobile ES users, which has been done last year. **propensity score matching** will be used to avoid selection bias and evaluate the effect of the treatment by comparing the treaded and non-treated group. It allows me to easily consider many independent variables at once, and it can be constructed using logistic regression. Multiple regression will also be used to examine the impact of users' attitudes towards perceived ES security. The research finding will help the security providers of ES to know the determinants of perceived security in the users' perspectives and to take measures to improve the determinants.

The remainder of the paper is constructed as follows. Section 2 describes the dataset, data collection, and exploratory data analysis on feature visualization. Section 3 outlines the data analysis models, which is designed to discover relationships between features and the target variable. Section 4 summarizes the model results according to evaluation criteria. Finally, Section 5 discusses the research findings and provides directions for future research.

This paper uses R statistical programming language (R Core Team 2020). In particular, we use packages `tidyverse` (Wickham et al. 2019), `here` (Muller 2020), `ggpubr` (Kassambara 2020) to manipulate data and packages, `kableExtra` (Zhu 2020) to generate tables, and `ggplot2` (Wickham 2016), `ggthemes` (Arnold 2021) to adjust diagrams themes.

2 Data

2.1 Intervention

To accomplish the research objectives, the author did a literature review on perceived security of mobile Enterprise System (ES). Based on the current research findings, the author concludes that there are five main categories of security issues when using mobile ES, which are mobile device issues, wireless network issues, cloud computing issues, application-level issues, and data access level issues. Different mobile phone users would have different attitudes and usage habits towards those five areas security issues, which greatly affect the perceived security of the ES. In order to test how different those impact on the iPhone and Android users, the author plan to divide people into two groups. The intervention of this research is using iPhone as mobile device. The treated group will be people who use iPhone (IOS) to operate the ES, and people in the control group will be those who use Android (Huawei, Samsung, Mi, and so on).

2.2 Data collection

An online questionnaire survey is the chosen method for collecting data from Mobile ES users. Compared with other methods, the major advantages of the online questionnaire are saving time, money, and manpower. Considering this research need to do a large quantity of data collection, the questionnaire is the only suitable method. The author conducted the online questionnaire survey one year ago under the guidance of the research method class.

Through the agency of Chinese online questionnaire platform 'Wenjuan Xing' and the researcher's personal relationship with certain companies, the author sends out around 800 online questionnaires randomly and 240 personal administered questionnaires. The personally administered survey is useful to increase the response rate and to enhance the data quality. The email reminders were sent for every ten days to encourage the potential participants to fill in their responses.

The respondents were asked to do a demographics survey which includes age, gender, occupation, years of experience, name of the ES systems used, functions or modules of Mobile ES, Brand of the mobile devices used to access the ES, and ownership of the device. The questionnaire also has items for measuring users' attitudes and usage habits on various security issues and perceived security of ES mobility. The data was collected by using an interval scale (0-strongly disagree to 10-strongly agree). The collected data was used for calculating the measures of central tendency (e.g. arithmetic mean), validating the hypotheses by using correlation, propensity score matching, multiple regression and other statistical analysis.

By the end of the survey period, data had been collected from 344 participants. As a result, the overall response rate is 33%. Among 344 responses, 13 responses were rejected on account of too much missing data. Therefore, 331 useable online questionnaire data were obtained and used for data analysis.

3 Model

```
## here() starts at /Users/yang/Downloads/Git/Security-of-Enterprise-System
```

3.1 T-test

3.2 correlation model

3.3 propensity score matching

3.4 regression model

4 Results

5 Discussion

5.1 First discussion point

5.2 Second discussion point

5.3 Third discussion point

5.4 Weaknesses and next steps

Weaknesses and next steps should also be included.

Appendix

A Additional details

References

Al Bar, Adnan, Essam Mohamed, Mohd Khursheed Akhtar, and Faris Abuhashish. 2011. "A Preliminary Review of Implementing Enterprise Mobile Application in Erp Environment." *International Journal of Engineering & Technology* 11 (4): 77–82.

Arnold, Jeffrey B. 2021. *Ggthemes: Extra Themes, Scales and Geoms for 'Ggplot2'.* https://CRAN.R-project.org/package=ggthemes.

Kassambara, Alboukadel. 2020. *Ggpubr: 'Ggplot2' Based Publication Ready Plots.* https://CRAN.R-project.org/package=ggpubr.

Matkerimov, T, and K Yakovlev. 2020. "Ways to Solve the Optimal Mobility of Forest Complex Machines in the Formation of a Logging Enterprise." In *IOP Conference Series: Earth and Environmental Science*, 595:012064. 1. IOP Publishing.

Muller, Kirill. 2020. *Here: A Simpler Way to Find Your Files.* https://CRAN.R-project.org/package=here.

R Core Team. 2020. *R: A Language and Environment for Statistical Computing.* Vienna, Austria: R Foundation for Statistical Computing. https://www.R-project.org/.

Rodrigues, Jorge, Pedro Ruivo, and Tiago Oliveira. 2021. "Mediation Role of Business Value and Strategy in Firm Performance of Organizations Using Software-as-a-Service Enterprise Applications." *Information & Management* 58 (1): 103289.

Siponen, Mikko T, and Harri Oinas-Kukkonen. 2007. "A Review of Information Security Issues and Respective Research Contributions." *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 38 (1): 60–80.

Wickham, Hadley. 2016. *Ggplot2: Elegant Graphics for Data Analysis.* Springer-Verlag New York. https://ggplot2.tidyverse.org.

Wickham, Hadley, Mara Averick, Jennifer Bryan, Winston Chang, Lucy D'Agostino McGowan, Romain François, Garrett Grolemund, et al. 2019. "Welcome to the tidyverse." *Journal of Open Source Software* 4 (43): 1686. https://doi.org/10.21105/joss.01686.

Zhu, Hao. 2020. *KableExtra: Construct Complex Table with 'Kable' and Pipe Syntax.* https://CRAN.R-project.org/package=kableExtra.