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

18 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.

2.3 Questionnaire design and sample

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 features

part will describe more about it. 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.

The screen shots of the questionnaire will be attached in the Appendix 1.

2.4 Dataset features

2.4.1 Demographics features

Overall, the dataset has 331 observations and contains 50 features. The first nine features describes users' demographic information.

- `Work_experience` : measures how long does the user work in the current company
- `Gender` : describes the user's gender
- `Age` : describes the user's age
- `Education_level` : describes user's educational level (High school, college, undergrad, postgrade)
- `Functions_used` : asks users which functionalities they use everyday
- `Usage_frequency` : describes the frequency of the usage of mobile ES
- `ES_Name` : describes the name of ES
- `Mobile_device` : asks for user's mobile phone brand
- `Device_ownership` : clarify if the mobile phone is owned by company or owned by the user

2.4.2 perceived ES security features [reference!!!]

The perceived ES security is this paper's dependent variable. According to Levent et al. (2005), enterprise security plan serves as an essential role to coordinate information security policies and applicable security technologies, making them align with the business rules and the developing information models and technical architectures. Consoli (2012) combined acknowledged definitions of context and security, and concluded the security context should point to five goals:Integrity to ensure that data is in the original format and not modified; Confidentiality to ensure that only authorized people have access to resources; Authentication for allowing the access to the resources; Availability to maintain the proper functioning of the information system; Non-repudiation to ensure that a transaction cannot be denied.

According to the definition above, the dataset has five features to measure the perceived ES security. Starting from here, the questionnaire is designed using interval scale (0-strongly disagree to 10-strongly agree). The user is asked to give a number between 0 and 10, which represent for their attitudes towards the given situation.

- `system_integrity` : measures user's attitude towards "I believe the data/ information in the mobile enterprise systems cannot be modified by unauthorized users"
- `system_availability` : measures user's attitude towards "I believe the data/ information in the mobile enterprise systems is available only to authorized users when required"
- `system_confidentiality` : measures user's attitude towards "I believe that the mobile enterprise systems are secured as the system detects and prevents the improper disclosure/ leakage of information"
- `system_accountability` : measures user's attitude towards "I believe that the mobile enterprise systems are secured as the system accounts the data changes"
- `system_nonrepudiation` : measures user's attitude towards "I believe that the mobile enterprise system is secured as the system does not deny any transaction that was carried out"

- `PSave` : (Dependent variable) used in the model. It takes a mean of the previous five features and presents for the user's perceived ES security.

2.4.3 Molibe device security issue features [references!!!]

A mobile device refers to any portable device which has computing and storage capabilities(Singh & Ranjan, 2016). The range of devices from smartphones, iPads, and tablets is quite popular among clients and IT professionals. Mobile users can work everywhere without being constrained by any networking system. These mobility and roaming features extend the network boundary beyond a single fixed point but make security management a much harder issue, because users cannot be tracked down into a fixed location anymore (Al Ladan, 2016). Moreover, mobile devices' operational systems are highly vulnerable, which results in threats having a variety of ways to spread. There is no device whose platform is completely closed, which has weakened the security performance of the original application and creates more risks for information sharing (Hermann & Fabian, 2014). There are six independent variables which might affect the perceived ES security:

- `Install_firewall` : measures user's attitude towards " I feel painful to install or update the security software such as antivirus and firewall software on my device."
- `BYOD` : measures user's attitude towards " I like the idea of using my own device for personal and corporate business."
- `Ignore_warnning` : measures user's attitude towards " I like to install applications in my mobile device without paying attention to permission warnings (or terms and conditions of usage)."
- `Strong_pin` : measures user's attitude towards " I feel painful to use a password or a pin code to lock my mobile device."
- `Store_passwords` : measures user's attitude towards " I feel it is simple and easy to store usernames and passwords on the device."
- `update_OS` :measures user's attitude towards " I feel painful to update the operating systems (e.g. iOS, Android) in my mobile device. "

2.4.4 Wireless network security issue features [reference!!!]

Mobile communication is generated mainly through radio signals rather than wires, so mobile ES has particular challenges compared with traditional computer-based ES. First of all, reliable Internet availability is a pre-requirement for the secure wireless network. According to Hermann and Fabian (2014), "the wireless network is more accessible to intercept and attack, so traditional security technologies such as firewalls, authentication servers, biometrics, cryptography, intrusion detection, and VPNs are not enough to address security issues in the wireless network"(Hermann & Fabian, 2014). There are six independent variables related to the wireless network which might affect the perceived ES security:

- `public_WiFi` : measures user's attitude towards " I believe it is secured to use the wireless networks in public places such as coffee shops, airport kiosks, or other hotspots"
- `unsecured_network` : measures user's attitude towards " I show no interest on the security threats on the wireless networks."
- `network_control` : measures user's attitude towards " I feel nervous to know the enterprise doesn't have much security control over the wireless networks."
- `network_attack` : measures user's attitude towards " I feel nervous to know that the hacker needs only a mobile device and a wireless card to capture data packets and transmission of the data."
- `encrypted_transimittion` : measures user's attitude towards " I believe the wireless network is not secured enough when the transmitted information is not encrypted."
- `unreliable_int` :measures user's attitude towards " I believe the data security and protection may be compromised when the Internet connection is not available and reliable. "

2.4.5 Cloud Computing Security Issue features

The appearance of cloud computing is narrowing down the gap between mobile ES and small to medium companies. Although it does cut down the set-up process time and cost and reduces the required skills in the company, some challenges and problems should still be kept in mind. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats (Picek, Mijac, & Androcec, 2017).There are six independent variables related to the cloud computing which might affect the perceived ES security:

- `cloud_resource` : measures user's attitude towards "I believe that the applications that use cloud resources are vulnerable to threats."
- `cloud_compute` : measures user's attitude towards "I believe the cloud computing is vulnerable for data security since the access can be interrupted at multiple points in the cloud."
- `remote_datastore` : measures user's attitude towards "Since the data is stored and processed remotely in cloud computing, I believe that the true ownership of the data becomes a security issue."
- `Data_regulation` : measures user's attitude towards "Since the data can be located anywhere in the world with different control and privacy regulations, I believe this practice leads to security risks."
- `multiple_login` : measures user's attitude towards " In a cloud environment, I like to logon to the same application using multiple devices simultaneously."
- `weak_authentication` :measures user's attitude towards "In a cloud environment, I like to use simple and short passwords."

2.4.6 Application level security issue features

The application-level mobile solution mainly consists of mobile operation systems and mobile applications. The application layer provides users with an interface to operate their mobile devices. The operation system act as a platform to run mobile applications. Application-level issues usually take place in a multi-tenant environment or in a virtualized world. There are six independent variables related to the application which might affect the perceived ES security:

- `unknown_app` : measures user's attitude towards "I feel pleasant to download applications from unreliable web sites or from links within e-mails"
- `update_ES` : measures user's attitude towards "I believe in installing updates for ERP systems to avoid any outdated security protections."
- `Auto_update` : measures user's attitude towards " I like to use automatic updater which applies any software application updates whenever available."
- `VPN` : measures user's attitude towards "I like to use VPN connections to download applications"
- `third_party_app` : measures user's attitude towards " I believe more fake apps/ malware versions (for Android) are found on third-party application sites."
- `update` :measures user's attitude towards "I like to update the device operating systems and applications when prompted."

2.4.7 Data Level Security Issue features

Since there is currently no appropriate regulation around data protection, data-level security is relying heavily on trust between the business and the provider. Data location and replication is one of the biggest concerns in the data level. A replica might be located in different countries where there is no clear legislation about data security and privacy, increasing the difficulty of managing the data (Kouatli, 2014). There are six independent variables related to the data access which might affect the perceived ES security:

- `single_authenticate` : measures user's attitude towards "I like single authentication process for data access using only passwords."

- `audit_log` : measures user's attitude towards "I dislike maintaining audit logs to track any changes in the data.."
- `access_right` : measures user's attitude towards "I feel comfortable to give access rights to access all information to all employees"
- `change_data` : measures user's attitude towards " I feel comfortable to give permission to change all information by all employees"
- `malicious_attack` : measures user's attitude towards " I believe hackers can harvest user information from mobile ES and create malicious content to fraud the individual user"
- `Data_threat` :measures user's attitude towards "I believe anytime and anywhere data access with ES mobility brings a large number of data security threats."

2.5 Descriptive Analysis

2.5.1 Treat distribution

From Figure 1 , we can clearly see that the iPhone user takes the lead and follows by HuaWei phone's user. One reason why iPhone is so popular is that The iPhone ensures all apps and functions are performing the way Apple intended them to perform, which allows for a very simple user experience. As we know, iPhone devices use IOS operation system, while other type of devices are mostly using Android operation system. So the the author category all the users into two groups, one is using IOS and the other one is using Android. The second graph shows a balanced state between all the respondents.

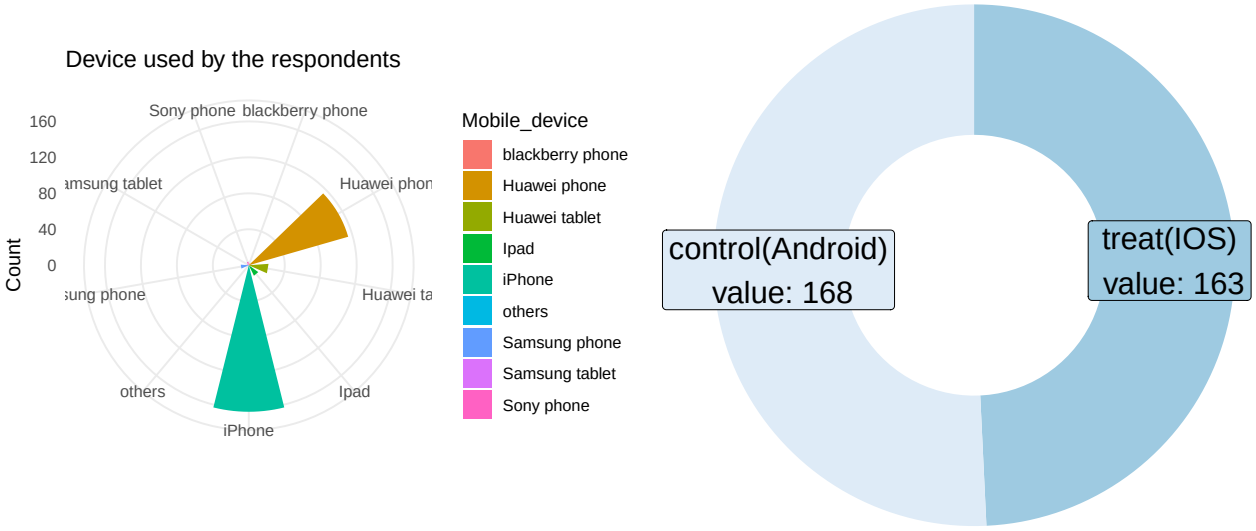

Figure 1: device used by the respondents

2.5.2 Demographics of user's work experience

Figure 2 demonstrates questionnaire respondents' work experience between treat group and control group. The red histogram represents people who use Android and the yellow histogram stands for iPhone users group. Working experience is an important element which might affect users' usage habits. The more professional they are, the more knowledge and experience they would have. Overall, we can see a relatively balanced match between iPhone and Android users. Most participants are holding three to five years working experience. It is interesting to find participants who has less than one year working experience like to use iPhone, while those with more than six year experience prefer to use Android. In terms of consistency, every

iPhone works the same, while every Android works differently. Maybe more professional people would like to customize their phone and have more power to control their device.

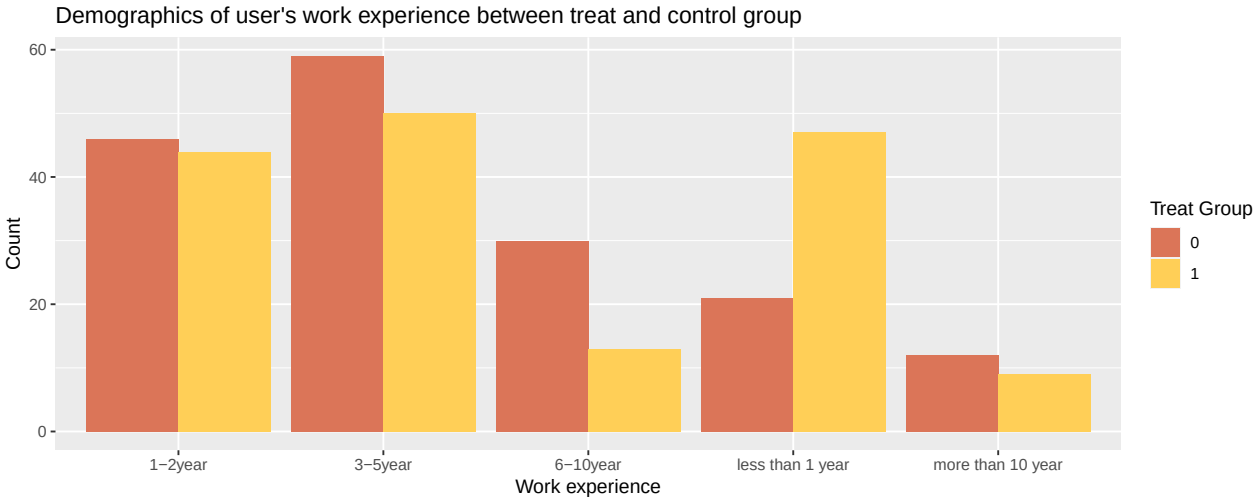

Figure 2: Demographics of user's work experience

2.5.3 Education level between treat and control group

Figure 3 uses the jitter plot to visualize the distribution of education level by intervention groups. As we can see from the chart, people's educational level is approximately at undergraduate and college. The iPhone user group is slightly more than Android user group in Master degree. But in general, there is not too much difference in terms of two group's educational level.

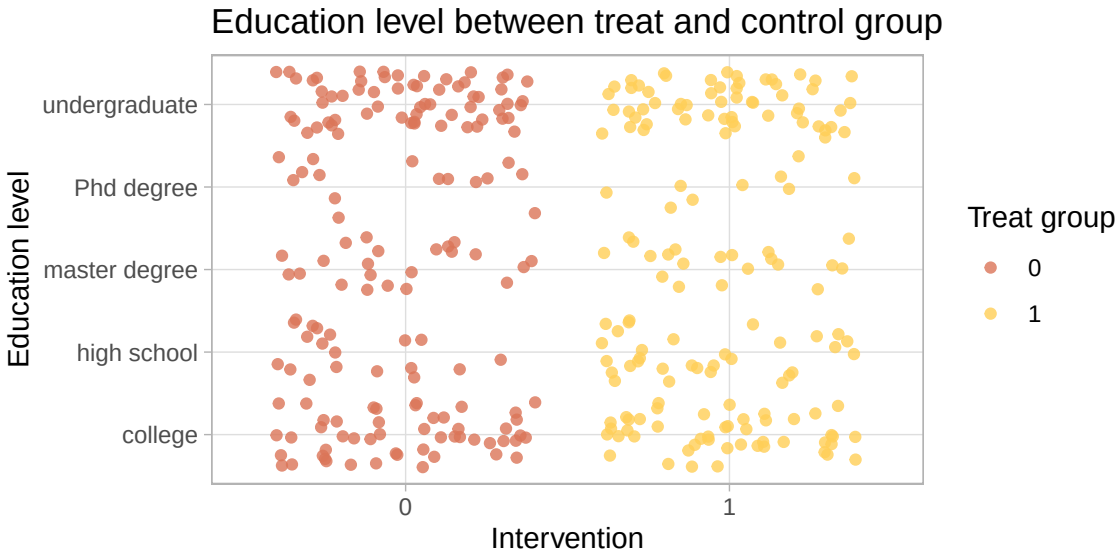

Figure 3: Education level between treat and control group

2.5.4 Device ownership

Device ownership also plays an important role in security context. Many employees bring their own device to the company for work and personal usage (bring your own device, BYOD), which is not trustworthy for enterprise system security (Souppaya and Scarfone 2013). As company has less control over employees' device, they have rights to download any software or choose the security level of their mobile devices. Figure 4 shows who own the device among 331 observations. We can find almost 95% devices are owned by the participants themselves.

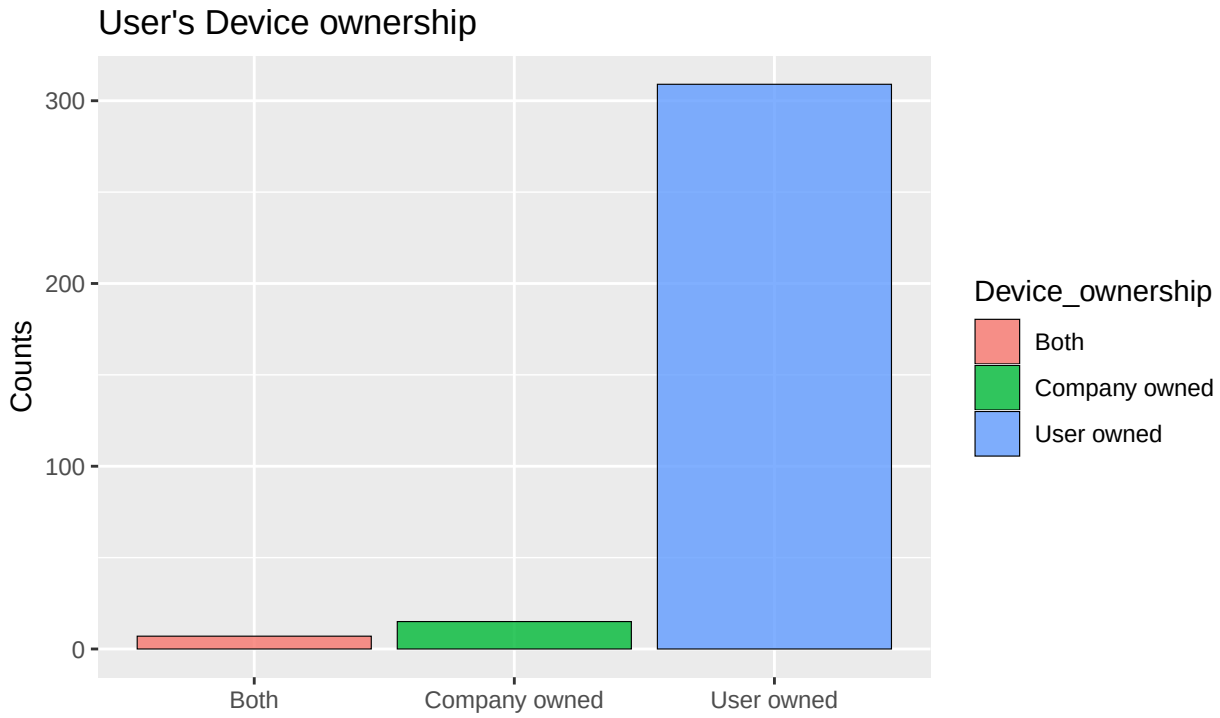

Figure 4: internet usages

3 Model

3.1 popensity score matching

3.2 Difference in means: outcome variable

3.3 T-test

We can carry out t-tests to evaluate whether these means are statistically distinguishable:

3.4 correlation model

3.5 propensity score matching

3.6 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.

Souppaya, Murugiah, and Karen Scarfone. 2013. "Guidelines for Managing the Security of Mobile Devices in the Enterprise." *NIST Special Publication* 800: 124.

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.