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

24 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

The perceived ES security is this paper's dependent variable. According to (Ertaul, Braithwaite, and Bellman 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 and others 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

A mobile device refers to any portable device which has computing and storage capabilities (Singh and 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 (Singh and Ranjan 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 and 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

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 and 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, and 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(Hermann and Fabian 2014). 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.

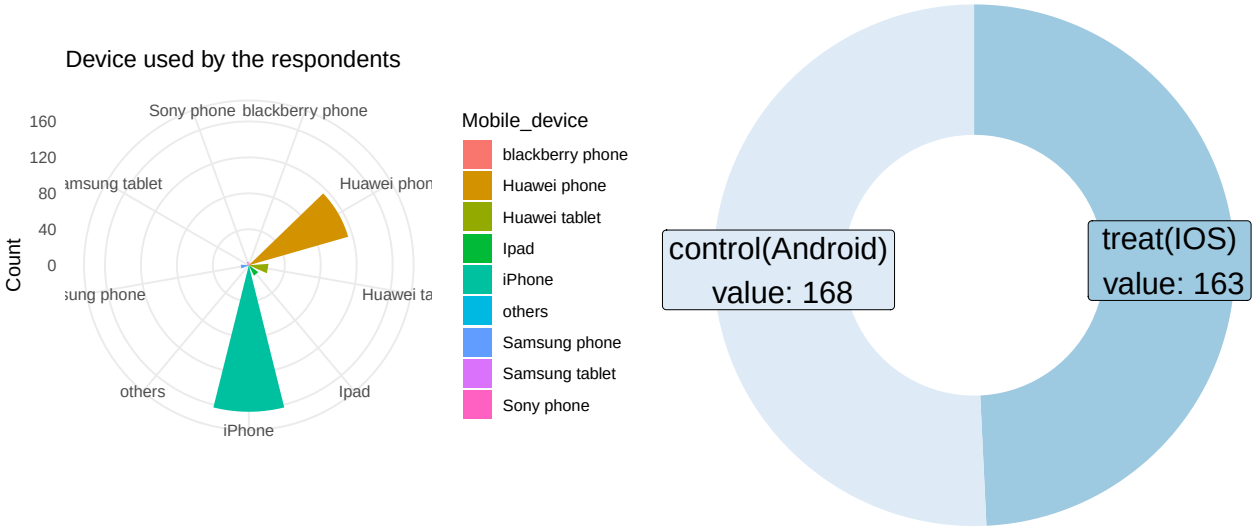

Figure 1: device used by the respondents

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.

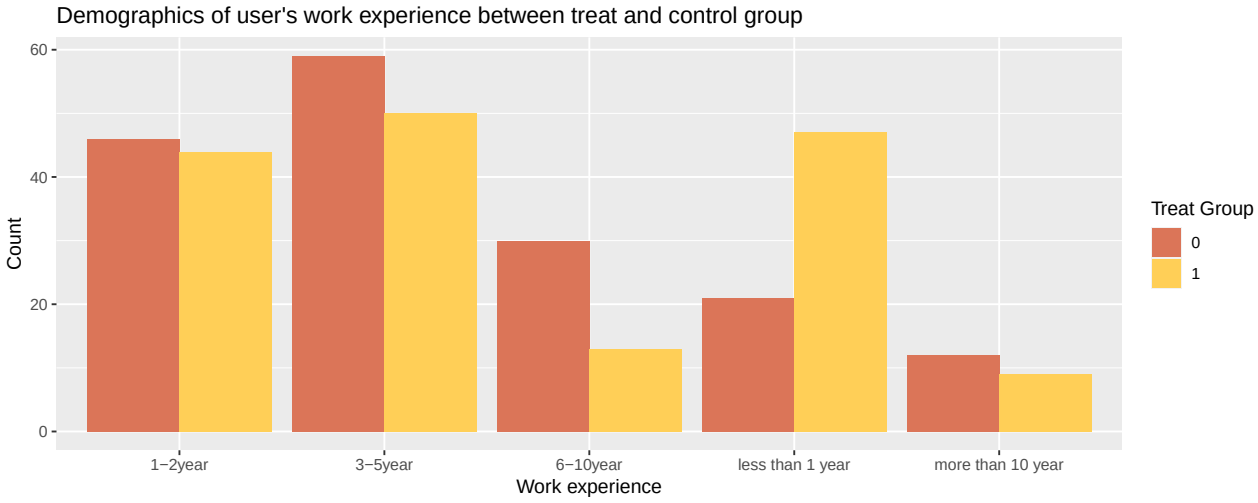

Figure 2: Demographics of user's work experience

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.

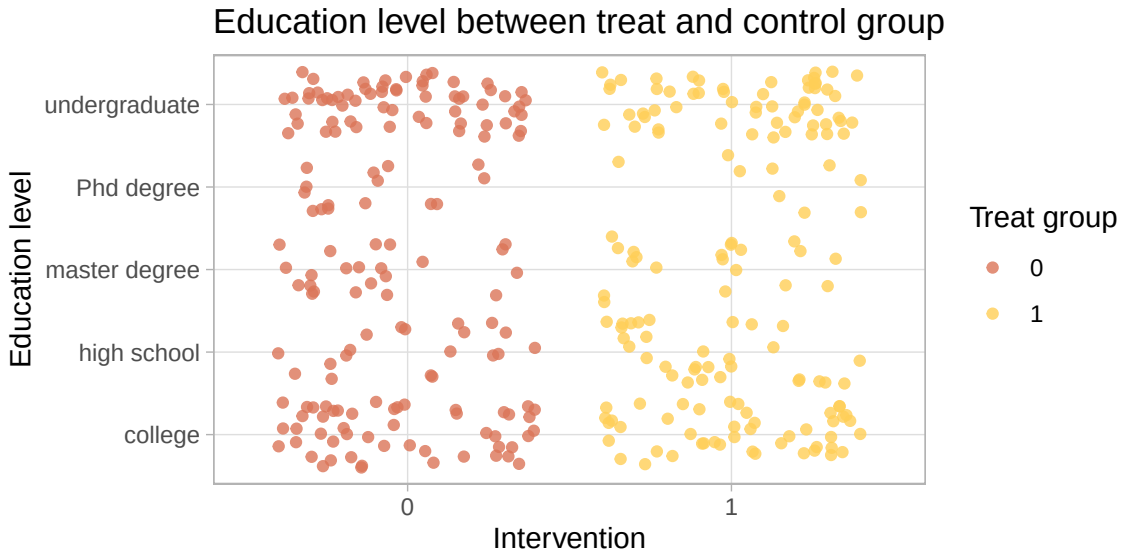

Figure 3: Education level between treat and control group

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.

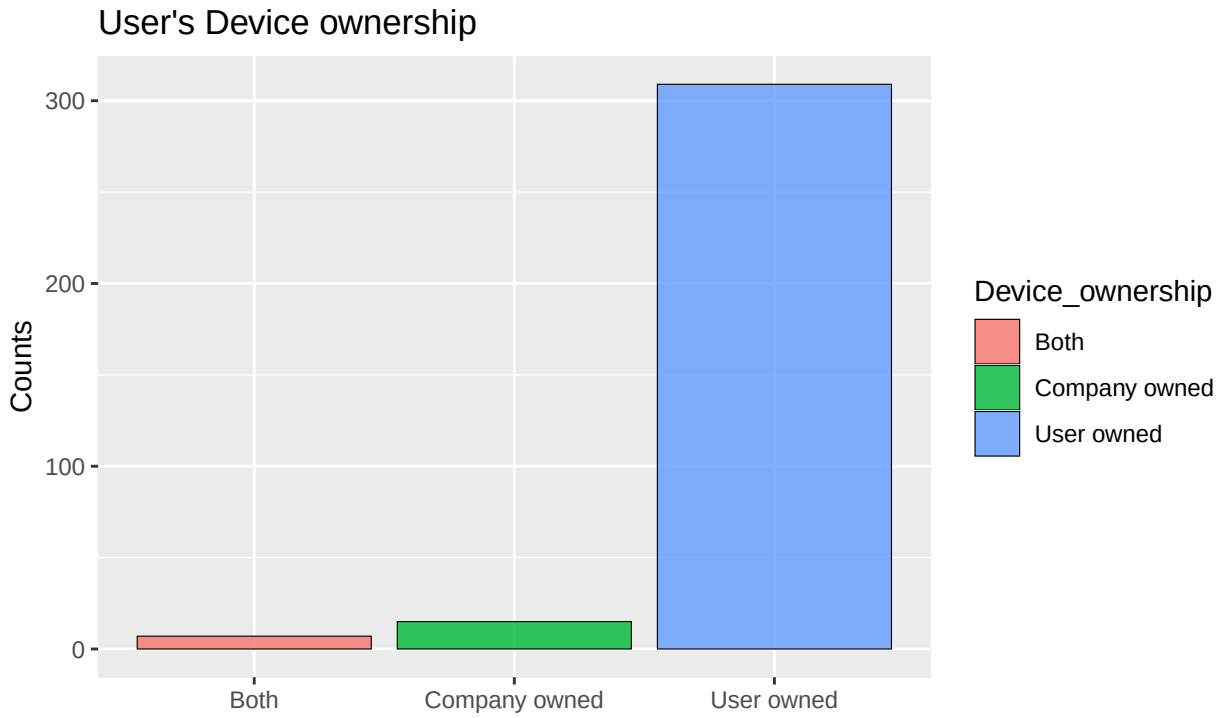

Figure 4: internet usages

3 Model

The author made a choice between difference in difference method and propensity score matching method. Both methods are good for analyze observation data. The difference-in-difference method captures the significant differences in outcomes across the treatment and control groups, which occur between pre-treatment and post-treatment periods(Lechner and others 2011). Difference in differences is a useful analysis framework to compare the changes in dependent variables, but in this project, it is hard to identify a certain time period. Because we cannot force our survey participants to use certain mobile devices in this period. Besides that, there might be a huge selection bias if we use DD method. Between iPhone and Android users, there would have lots of difference like their education level, age, gender, work experience and so on. It is really hard to match the people in the treat and control groups as closely as possible. Therefore, the author choose to use propensity score matching in this project.

3.1 propensity score matching method

Propensity score matching estimators are widely used in evaluation research to estimate average treatment effects(Abadie and Imbens 2016). Propensity score matching creates a group of participants for the treatment

and control groups. The matching group consists of at least one participant in the treatment group with similar propensity scores and at least one participant in the control group. The goal is to approximate a random experiment and eliminate many problems caused by observational data analysis like selections bias.

3.2 propensity score estimation

Basically, the propensity score matching method would assign some probability to each observation. In this project, based on the independent variables (users' attitudes towards different kind of security issues), the author constructs the propensity score estimation. We estimate the propensity score by running a logit model where the dependent variable (perceived ES security) is a binary variable indicating treatment status. **glm()** is used to fit generalized linear models, specified by giving a symbolic description of the linear predictor and a description of the error distribution(Simon et al. 2011). Table 1 shows the results. We can then compare the outcomes of observations with similar propensity scores.

Table 1: propensity score estimation table

	Model 1
(Intercept)	1.373**
	(0.684)
Install_firewall	-0.035
	(0.144)
BYOD	0.112
	(0.154)
Ignore_warnning	-0.100
	(0.105)
Strong_pin	0.039
	(0.101)
Store_passwords	-0.047
	(0.110)
update_OS	0.027
	(0.129)
public_WiFi	0.003
	(0.115)
unsecured_network	-0.107
	(0.133)
network_control	0.256
	(0.163)
network_attack	0.060
	(0.153)
encrypted_transimittion	0.050
	(0.097)
unreliable_int	-0.094
	(0.139)
cloud_resource	-0.124
	(0.138)
cloud_compute	0.089
	(0.167)
remote_datastore	-0.037
	(0.151)
Data_regulation	-0.092
	(0.190)
multiple_login	0.008
	(0.195)
weak_authentication	0.219
	(0.149)
unknown_app	0.284**
	(0.127)
update_ES	-0.164
	(0.150)
Auto_update	-0.353**
	(0.141)
VPN	0.325*
	(0.170)
third_party_app	-0.192
	(0.159)
update	-0.110
	(0.146)
single_authenticate	-0.247*
	(0.138)
audit_log	0.395**
	(0.190)
access_right	-0.064
	(0.170)
change_data	0.001
	(0.157)
malicious_attack	-0.303**
	(0.146)
Data_threats	-0.068
	(0.157)
Num.Obs.	331
AIC	473.0
BIC	590.8
Log.Lik.	-205.477

* p < 0.1, ** p < 0.05, *** p < 0.01

Using this model, we can now calculate the propensity score for each ES user. It is simply the user's predicted probability of being Treated, given the estimates from the logit model. Below, the author calculates this propensity score using **predict()** and create a dataframe that has the propensity score as well as the user's actual treatment status. Table 2 shows the first 6 rows of result.

Table 2: ES user's propensity score and actual treatment status

pr_score	treat
0.1919596	0
0.5073056	1
0.4182058	0
0.1465885	1
0.2038893	0
0.0506724	1

3.3 Examing the Region of common support

After estimating the propensity score, it is useful to plot histograms of the estimated propensity scores by treatment status. As shown in Figure 5, these graphics show the overlap of the propensity scores of the two groups, suggesting they share a lot of common support on the covariates in the model.

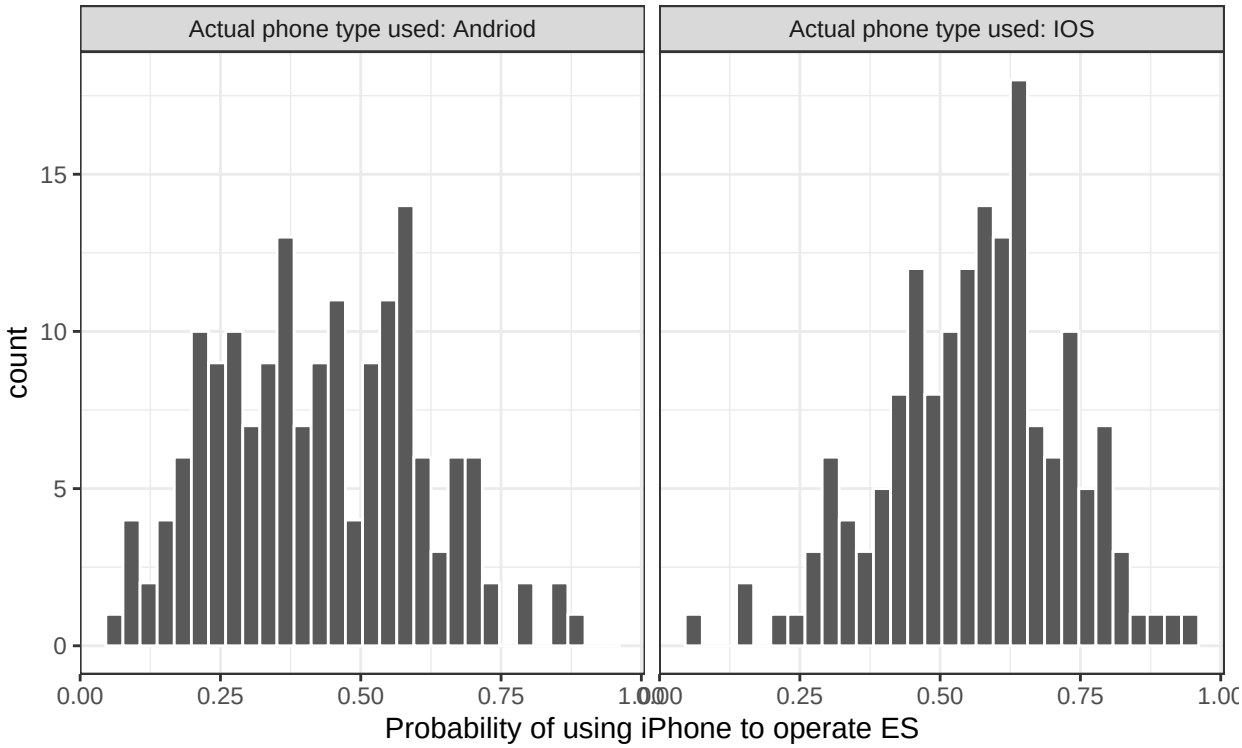

Figure 5: ES user's propensity score

Common support Figure 6 indicates the regions of stratification share enough members of the treatment and control groups.

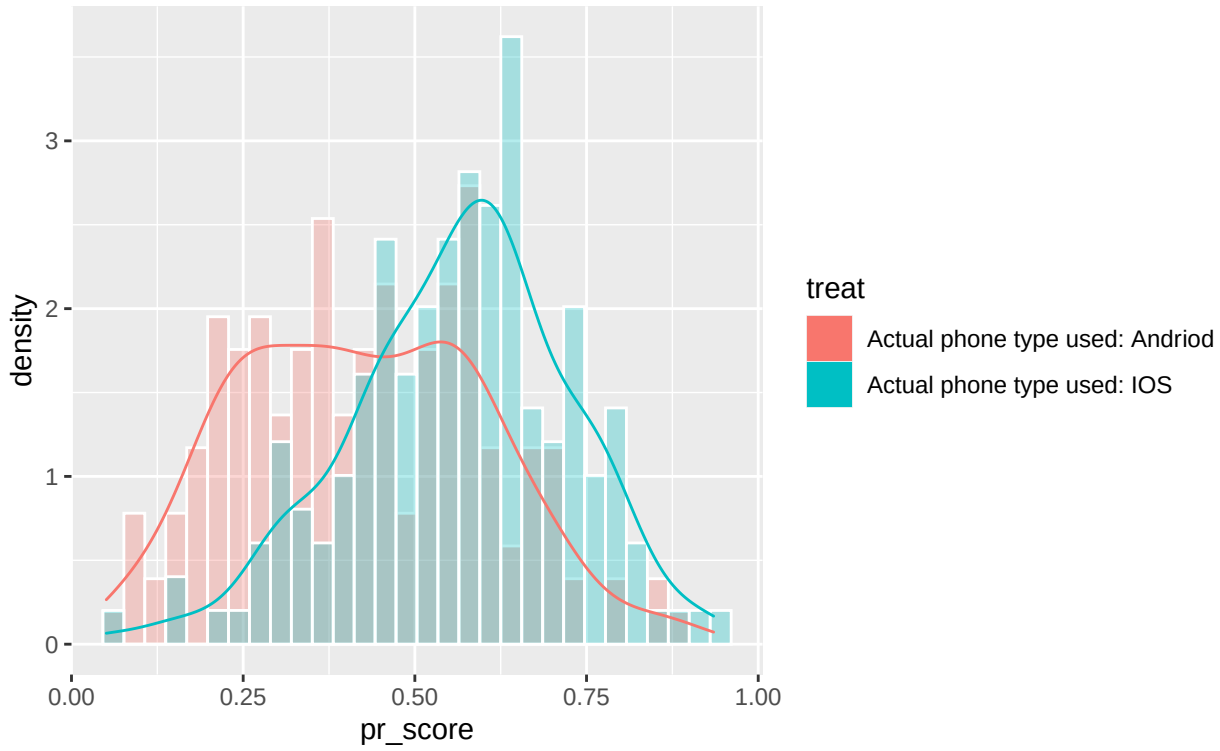

Figure 6: ES user's propensity score

3.4 Executing matching algorithm

MatchIt package (Ho et al. 2011) is used here to find pairs of observations that have very similar propensity scores, but that differ in their treatment status. This package estimates the propensity score in the background and then matches observations based on the "nearest" method.

Note that the final dataset is smaller than the original: it contains 326 observations, meaning that 163 pairs of treated and control observations were matched. Also note that the final dataset contains a variable called distance, which is the propensity score.

Table 3: Head of raw matching dataset

3.5 Model check—Examining covariate balance in the matched sample

The author uses visualization to show whether the matching is done well. The Figure 7 plots the mean of each independent variable against the estimated propensity score, separately by treatment status. If the matching result is good, the treatment and control groups will have similar identical means of each covariate at each value of the propensity score. In general, the model has a good match.

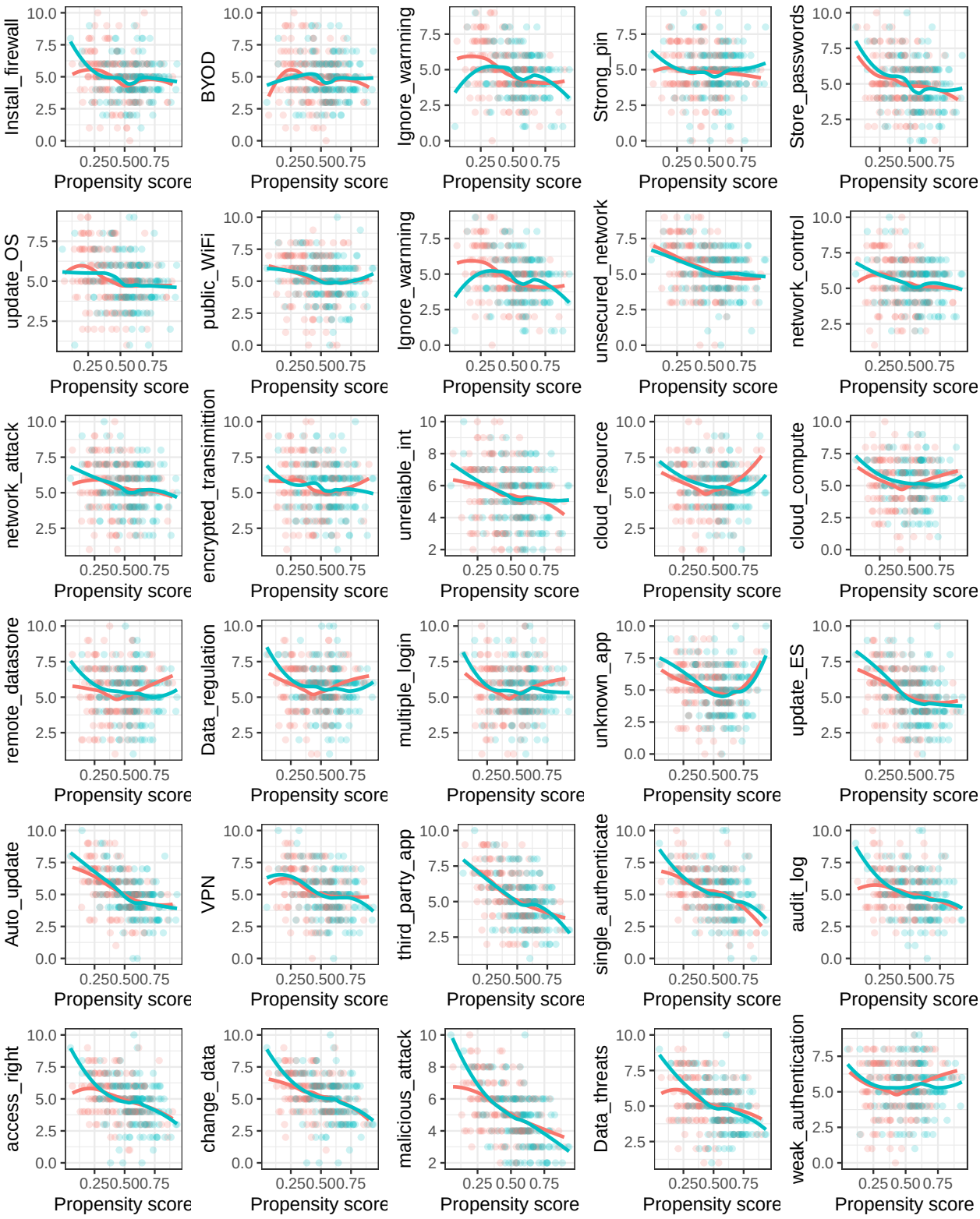

Figure 7: covariate balance check

3.6 Estimating treatment effects—T-test

The t-test is used to compare the sample mean of our Treated group(IOS) and Control group(Android). The goal is to determine whether the intervention has an effective effect on the treated group. Our hypothesis is that the intervention will increase the perceived ES security. The t-test results will be presented in the next section. The package **Broom** (Robinson, Hayes, and Couch 2021) is used to clean the t test results and convert it into the dataframe.

3.7 Estimating treatment effects—regression model

We are using RStudio to run the multiple linear regression model. The following reasons explain why we decide to choose multiple linear regression to test the treatment effects (Weedmark 2021):

- It account for all of the potentially important factors in one model
- It leads to a more precise understanding of the relationship between dependent variables and independent variables
- It is able to identify outliers or anomalies in the dataset.

R squared :

R-squared is a measure of the goodness of fit of the model. A larger R-squared indicates a closer fit of the model to the data. It is used as an optimality criterion in parameter selection and model selection (Johansen 1980).

P-value:

P-value is used to describe the occurrence possibility of the extreme outcome when the null hypothesis is true (Ioannidis 2018). If the p-value is small, it means that the probability of occurrence of the null hypothesis to be true is very small. And if it does occur, we have a reason to reject the null hypothesis. In short, the smaller the p-value, the more significant the result. Usually the threshold for significant p value is set to 0.05.

Regression coefficient:

The sign of the regression coefficient describes whether there is a positive or negative correlation between each feature variable and the dependent variable (Warren affective score). A positive coefficient means that as the value of the independent variable increases, the average value of the affective score also tends to increase. A negative coefficient indicates that as the independent variable increases, the affective score tends to decrease (Uyanık and Güler 2013).

4 Results

4.1 Correlation matrix

Correlation matrix shows internal relationships between users' attitude feature variables and our variable of interest, perceived ES security. (Figure 8) Intensity and direction of relationship is indicated by the color scale from red to blue (+1 to -1. descendant). Insignificant coefficient is barred with symbol "x". From the correlation matrix below, it is evident that the dependent variable (PSave) has secure connections with the independent variables.

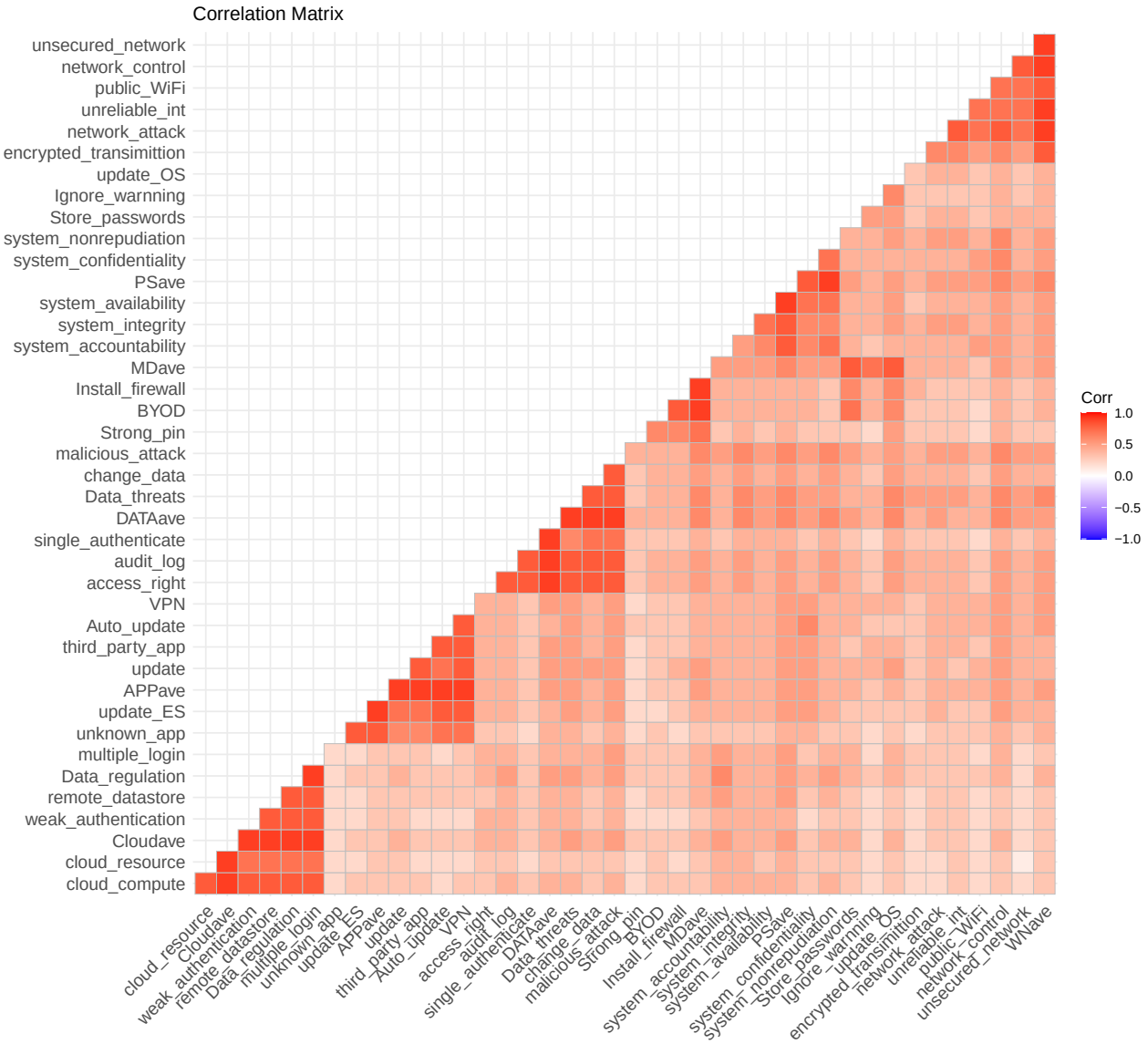

Figure 8: Correlation matrix

4.2 Two-sample T-test results

4.2.1 Average perceived ES security score

Table 4 shows some basic statistic analysis about iPhone group and Android group. The average perceived ES security for iPhone group is 5.082209. The average perceived ES security for Android group is 5.427381.

The standard error is considered part of inferential statistics. It represents the standard deviation of the mean within a dataset. This serves as a measure of variation for random variables, providing a measurement for the spread. The smaller the spread, the more accurate the dataset. The standard error is 0.1227353 for control group and 0.1076873 for treat group.

Table 4: Difference-in-means: dependent variable

treat	n_users	mean_perceived_security	std_error
0	168	5.427381	0.1227353
1	163	5.082209	0.1076873

4.2.2 T-test results

After propensity score matching, Table 5 shows the t-test result. The p value we get is 0.073385, as the p value would indicate a significant difference between two groups (a typical threshold is 0.05, anything smaller counts as statistically significant). The 95% confidence interval shows that the true difference is between -0.0280458 and 0.6170028.

Table 5: T-test on dependent variable

estimate1	estimate2	p.value	conf.low	conf.high	method	alternative
5.376687	5.082209	0.073385	-0.0280458	0.6170028	Welch Two Sample t-test	two.sided

4.3 Model Results

Multiple linear regression was applied to predict the perceived ES security, using 30 independent variables and 1 1 dummy variable which indicate the intervention status.

4.3.1 Treatment effect result

Table 6 shows the treatment effect. In this model result, the intercept (5.377) represents the average effect for the reference group. There is only one reference group : **Treat: treat 0 (using Android devices)**The coefficient for **treatment effect** is -0.294, suggesting that the average perceived security from people who use iPhone is on average 0.294 unit lower than those who use Android, holding other variables constant. The p value is 0.0734, which indicates this is a significant result.

Table 6: Treatment effect

	Model 1
(Intercept)	5.377***
	(0.116)
treat1	-0.294*
	(0.164)
Num.Obs.	326
R2	0.010
R2 Adj.	0.007
AIC	1184.7
BIC	1196.1
Log.Lik.	-589.358
F	3.227

* p < 0.1, ** p < 0.05, *** p < 0.01

4.3.2 regression model results

As shown in the summary table,Table 7[1], there are 7 variables are significant (p<0.05) to the perceived ES security: update_OS; network_control; Data_regulation; weak_authentication; public_WiFi; Auto_update; malicious_attack.

[1]The 'modelsummary' package Arel-Bundock (2021) was helped to create the table.

The coefficient for **updata_OS** is 0.156, suggesting that one unit increase in updata_OS score is associated with 0.156 unit increase in the perceived ES security, holding other variables constant.The p value is 0.005613, which indicates this is a significant result.

The coefficient for **public_wifi** is 0.133, suggesting that one unit increase in public_wifi score is associated with 0.133 unit increase in the perceived ES security, holding other variables constant.The p value is 0.011162, which indicates this is a significant result.

The coefficient for **network_control** is 0.232, suggesting that one unit increase in network_control score is associated with 0.232 unit increase in the perceived ES security, holding other variables constant.The p value is 0.001147, which indicates this is a significant result.

The coefficient for **Data_regulation** is 0.307, suggesting that one unit increase in data regulation score is associated with 0.307 unit increase in the perceived ES security, holding other variables constant.The p value is 0.000398, which indicates this is a significant result.

The coefficient for **Auto_update** is 0.132, suggesting that one unit increase in Auto_update score is associated with 0.132 unit increase in the perceived ES security, holding other variables constant.The p value is 0.036760, which indicates this is a significant result.

The coefficient for **malicious_attack** is -0.303, suggesting that one unit increase in malicious_attack score is associated with 0.303 unit decrease in the perceived ES security, holding other variables constant.The p value is 0.000902, which indicates this is a significant result.

The coefficient for **weak_authentication** is -0.155, suggesting that one unit increase in weak_authentication score is associated with 0.155 unit decrease in the perceived ES security, holding other variables constant.The p value is 0.021122, which indicates this is a significant result.

Table 7: Regression results summary table

	Model 1
(Intercept)	-0.042
	(0.306)
Install_firewall	-0.020
	(0.062)
BYOD	0.008
	(0.064)
Ignore_warnning	0.038
	(0.046)
Strong_pin	0.044
	(0.046)
Store_passwords	0.015
	(0.047)
update_OS	0.156***
	(0.056)
public_WiFi	0.133**
	(0.052)
unsecured_network	-0.031
	(0.059)
network_control	0.235***
	(0.070)
network_attack	-0.076
	(0.068)
encrypted_transimittion	0.001
	(0.043)
unreliable_int	0.036
	(0.062)
cloud_resource	0.022
	(0.062)
cloud_compute	0.077
	(0.073)
remote_datastore	0.065
	(0.066)
Data_regulation	0.306***
	(0.086)
multiple_login	-0.102
	(0.085)
weak_authentication	-0.153**
	(0.067)
unknown_app	-0.016
	(0.053)
update_ES	0.096
	(0.067)
Auto_update	0.128**
	(0.062)
VPN	-0.056
	(0.075)
third_party_app	-0.020
	(0.071)
update	-0.018
	(0.066)
single_authenticate	0.026
	(0.060)
audit_log	-0.103
	(0.083)
access_right	0.033
	(0.076)
change_data	0.006
	(0.070)
malicious_attack	0.219***
	(0.066)
Data_threats	-0.048
	(0.069)
Num.Obs.	326
R2	0.625
R2 Adj.	0.587
AIC	925.9
BIC	1047.1
Log.Lik.	-430.935
F	16.415

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$

The summary table above shows that the R-square value for the multiple linear regression model is 0.626, which means about 62.6% of the variation in the dependent variable(perceived ES security) can be explained by the multiple linear regression model.

5 Discussion

In a short conclusion, this research posts a question at the beginning: will iPhone user be more secure than Android user when using mobile enterprise system? To answer this question, the author did a literature review and category five main security issues when using mobile app. Based on that, the data was collected through the online questionnaire survey. The dataset was divided into two groups (IOS group and Android group), propensity score matching was applied to avoid selection bias. Though the treatment effect (iPhone as device) is not significant, we can not tell there is a strong evidence to support iPhone user is more secure than Android user when using mobile ES. The author still find something interesting about the dataset features. Through the multiple linear regression model, the author examined the impact of users' attitude towards security issues on perceived security of ES mobility. The study findings will be used to evolve strategic considerations for designing and developing secured mobile ES. This will help the security providers of ES to know the determinants of perceived security in the users' perspective and to take measures to improve the determinants.

5.1 Causality

Through the multiple linear regression, the treatment effect (treat1) is -0.294, which means using iPhone as device to operate enterprise system would be less secured than using Android. The p value is 0.07, which provide a strong evidence to support the regression result. Our guess that iPhone user would be more secured is rejected. In other word, using Android device would increase the perceived ES security. Android users have better awareness to defend different security issues.

5.2 Research findings

5.2.1 Android user's average perceived ES security is higher!

From the result of the two sample T test, we are amazed to find the score for Android user's average perceived ES security is around 6% higher than iPhone user's score. The sample distribution shows employees who have more than 3 years working experience more inclined to use Android phones. While for those employees with less than 1 year working experience, they are the majority iPhone users. Android users has better awareness towards the security issues might have the following reasons: Apple think what is the best for you, and no matter what you need or not. So iPhone locks down the UI and system setting, which greatly limit the customization. In contrast, users can make their Android phone unique! With deep knowledge, users can make their Android phone more secured.

5.2.2 Wireless network security issues have the most critical impact

According to the multiple linear regression model result, the regression coefficients for "public_WiFi", and "network_control" are very significant, indicating that users' attitudes towards wireless network security issues have the most critical impact on the perceived system security.

(Zissis and Lekkas 2012) explained that the perceived security of ES mobility refers to three fundamental properties: confidentiality, integrity, and availability. Each of the three dimensions would be attacked when mobile devices are connecting with the wireless network. Confidentiality attack happens when location-less hacker destroys or steals users' information through the radio signals; integrity attack happens when a hacker compromises the wireless network to modify, exchange or retransmit enterprise data; and availability attack happens when service availability is disrupted (Leung, Sheng, and Cruickshank 2007).

Compared with the wired network, the wireless context is more vulnerable to be hacked because the transmission method of the radio signal is exposed to the air and could be intercepted anytime and anywhere. Besides, the wireless network is usually provided by a private service provider and operated on public shared

infrastructure. The majority of small to medium enterprises do not have rights to control or manage the wireless network security setting, and they also lack of knowledge about security of the network infrastructure (Zissis and Lekkas 2012). After analyzing the implications of finding, the following best practices for addressing users' attitudes towards wireless network security issues are listed:

- Do not use public Wi-Fi to operate any mobile Enterprise system (such as Wi-Fi in coffee shops, airport kiosks or other hotspots).
- Pay attention to wireless network security warnings that pop up on mobile devices
- Keep your web browser, wireless firewall, and anti-virus software up to date.

5.2.3 Business need a strategic level security plan toward ES mobility

Through the demographics of ownership of the device, it is notable to find that 93 percent of mobile devices are owned by users. "Bring your own device" (BYOD) issues increase the risk of data breaches because the portable devices are easy to get lost or stolen (He 2013). Besides, when employees leave the organization, they are no longer under the protection of the company's network's firewall. However, the company's confidential data is still stored in that device. Accordingly, BYOD will increase the possibility of data leaking, and it is more vulnerable for malicious threats. Companies can cause security crises if their employees lack an understanding of the different changes in the enterprise security environment. Many mobile users overly trust the security of their device and often ignore security alerts. For example, many users do not care about the permission warnings before installing the applications(He 2013). Based on that, the author put forwards the following advice:

- It is vital for any business to have a strategic level security plan toward ES mobility.
- Pay attention to permission warnings (or terms and conditions of usage) when installing the applications
- The mobile ES user should involve themselves in developing an enterprise-level security plan and understand how it works.

5.3 Weaknesses and next steps

5.3.1 potential limitations

First, there are a considerable number of mobile ERP users distributed all over the world. However, the questionnaire survey in this study was only carried out in China. In addition, the sample overrepresents the female perspective (57%) and the perceptive of the iPhone mobile user (53%). The sample is not entirely representative of the wide range of mobile ES users. These limitations could bias the results of the data analysis.

Second, the number of respondents for the questionnaire survey is not large enough, which might lower the universality of the research results.

Third, this study uses the online questionnaire as its method to collect data, and the accuracy and quality of the data cannot be guaranteed because of participants' perfunctory responses.

Fourth, The true propensity score is never known in observational studies, so you can never be certain that the propensity score estimates are accurate (Abadie and Imbens 2016). Some authors urge caution in knowing the limitations of what really amounts to an estimation tool, they mentioned that "trying to approximate a random experiment from observational data can be fraught with pitfalls" (Caliendo and Kopeinig 2008).

5.3.2 Future research direction

This research aims to find how different iPhone users act compared with Android users, and how those actions or awareness impact the perceived ES security. Unfortunately, the treatment effect is not obvious.

This study also focuses on users' attitudes on the perceived security of enterprise systems mobility. In order to enhance the security of mobile ERP software, IT developers are also essential for system maintenance. Future research could study how to increase system security and reduce risks from the perspective of IT staff.

The data collection can be done in the perspective of IT staff and top management. In addition, to avoid limitations on the sample, the future researchers can consider carrying out investigations with respondents from a broader scope and more diverse backgrounds, which can help enhance the universality and quality of the data collection.

Appendix

A Additional details

References

Abadie, Alberto, and Guido W Imbens. 2016. "Matching on the Estimated Propensity Score." *Econometrica* 84 (2): 781–807.

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.

Arel-Bundock, Vincent. 2021. *Modelsummary: Summary Tables and Plots for Statistical Models and Data: Beautiful, Customizable, and Publication-Ready*. https://CRAN.R-project.org/package=modelsummary.

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

Caliendo, Marco, and Sabine Kopeinig. 2008. "Some Practical Guidance for the Implementation of Propensity Score Matching." *Journal of Economic Surveys* 22 (1): 31–72.

Consoli, Domenico, and others. 2012. "A Corporate Security Strategy in an Enterprise 2.0 Model." *Managerial Challenges of the Contemporary Society*, no. 3: 102–6.

Ertaul, Levent, Timothy Braithwaite, and Beryl L Bellman. 2005. "Enterprise Security Planning (Esp)." In *Proceedings of Euro mGOV*. Vol. 2005.

He, Wu. 2013. "A Survey of Security Risks of Mobile Social Media Through Blog Mining and an Extensive Literature Search." *Information Management & Computer Security*.

Hermann, Steffen, and Benjamin Fabian. 2014. "A Comparison of Internet Protocol (Ipv6) Security Guidelines." *Future Internet* 6 (1): 1–60.

Ho, Daniel E., Kosuke Imai, Gary King, and Elizabeth A. Stuart. 2011. "MatchIt: Nonparametric Preprocessing for Parametric Causal Inference." *Journal of Statistical Software* 42 (8): 1–28. https://www.jstatsoft.org/v42/i08/.

Ioannidis, John PA. 2018. "The Proposal to Lower P Value Thresholds to. 005." *Jama* 319 (14): 1429–30.

Johansen, Søren. 1980. "The Welch-James Approximation to the Distribution of the Residual Sum of Squares in a Weighted Linear Regression." *Biometrika* 67 (1): 85–92.

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

Kouatli, Issam. 2014. "A Comparative Study of the Evolution of Vulnerabilities in It Systems and Its Relation to the New Concept of Cloud Computing." *Journal of Management History*.

Lechner, Michael, and others. 2011. *The Estimation of Causal Effects by Difference-in-Difference Methods*. Now.

Leung, Adrian, Yingli Sheng, and Haitham Cruickshank. 2007. "The Security Challenges for Mobile Ubiquitous Services." *Information Security Technical Report* 12 (3): 162–71.

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.

Picek, Ruben, Marko Mijac, and Darko Androcec. 2017. "Acceptance of Cloud Erp Systems in Croatian Companies: Analysis of Key Drivers and Barriers." *Economic and Social Development: Book of Proceedings*, 513–22.

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

Robinson, David, Alex Hayes, and Simon Couch. 2021. *Broom: Convert Statistical Objects into Tidy Tibbles.* https://CRAN.R-project.org/package=broom.

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.

Simon, Noah, Jerome Friedman, Trevor Hastie, and Rob Tibshirani. 2011. "Regularization Paths for Cox's Proportional Hazards Model via Coordinate Descent." *Journal of Statistical Software* 39 (5): 1–13. https://www.jstatsoft.org/v39/i05/.

Singh, Archana, and Jayanthi Ranjan. 2016. "A Framework for Mobile Apps in Colleges and Universities: Data Mining Perspective." *Education and Information Technologies* 21 (3): 643–54.

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.

Uyanık, Gülden Kaya, and Neşe Güler. 2013. "A Study on Multiple Linear Regression Analysis." *Procedia-Social and Behavioral Sciences* 106: 234–40.

Weedmark, David. 2021. "The Advantages & Disadvantages of a Multiple Regression Model." 2021. https://sciencing.com/advantages-disadvantages-multiple-regression-model-12070171.html.

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.

Zissis, Dimitrios, and Dimitrios Lekkas. 2012. "Addressing Cloud Computing Security Issues." *Future Generation Computer Systems* 28 (3): 583–92.