applied sciences

MDPI

Article

Predictors of Employees' Mobile Security Practice: An Analysis of Personal and Work-Related Variables

Zauwiyah Ahmad [1], Thian Song Ong [2,*], Yen Wen Gan [2], Tze Hui Liew [2] and Mariati Norhashim [3]

[1] Faculty of Business, Multimedia University, Jalan Ayer Keroh Lama, Melaka 75450, Malaysia; zau@mmu.edu.my
[2] Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, Melaka 75450, Malaysia; ganyenwen.0905@gmail.com (Y.W.G.); thliew@mmu.edu.my (T.H.L.)
[3] Faculty of Management, Multimedia University, Persiaran Multimedia, Cyberjaya 63100, Malaysia; mariati.norhashim@mmu.edu.my
* Correspondence: tsong@mmu.edu.my

Abstract: Personal mobile devices form an integral part of business activities today. Mobile devices, nevertheless, pose various security issues and data privacy threats, which require a close attention. The rational choice theory was utilized to examine the determinants of employees' security behavior in relation to mobile device usage. Employees were postulated to rationally evaluate the costs and benefits of mobile security measures and decide on the option that is perceived to provide the best expected outcome. Twelve out of thirteen hypotheses examined in this study were found to be significant. We also hypothesized that demographics and work-related variables significantly affect employees' mobile security practices, examined using ordinal logistic regression analysis. The findings indicate the efficacy of the rational choice theory in explaining mobile security behavior. Security inconvenience has been found to be a significant cost to information security measures. Moreover, the findings also showed the influence of gender, job function, past security experience, and perceived risk on the dependent variable. In conclusion, we would like to draw considerable attention to the contribution of security awareness programs and security training to good mobile security behaviors.

Keywords: mobile security; data privacy; security awareness; cost–benefit analysis; rational choice theory

check for updates

Citation: Ahmad, Z.; Ong, T.S.; Gan, Y.W.; Liew, T.H.; Norhashim, M. Predictors of Employees' Mobile Security Practice: An Analysis of Personal and Work-Related Variables. *Appl. Sci.* **2022**, *12*, 4198. https://doi.org/10.3390/app12094198

Academic Editor: Gianluca Lax

Received: 17 February 2022
Accepted: 6 April 2022
Published: 21 April 2022

1. Introduction

Technological advancement has induced a parallel change in the work environment, specifically, the widespread use of mobile devices for work purposes, which has formed an integral part of today's business operations by supporting operational efficiency and productivity. Organizations have been found to allow employees to use any device to connect to the organization's network [1], and the practice may expose organizations to information security threats.

The use of mobile devices that are not monitored by the organization for work purposes could cause various security issues. Among reported issues are (1) malicious apps downloaded onto a mobile device; (2) lost or stolen mobile devices that contain sensitive or proprietary data; (3) concerns regarding data ownership, especially during the resignation of the employee, (4) access of sensitive corporate data via untrusted or public networks; and (5) failure to implement access control on mobile devices [2–4]. Moreover, Hayes et al. [5] determined that mobile applications collect extensive amounts of data without user consent or knowledge, and this is contrary to the developers' privacy policies.

What is more concerning is, in spite of these security issues, employees believe that they have none to very little responsibility to safeguard the organizational data stored on their mobile devices [3,4]. Mobile device users generally underestimate the threats and risks associated with the use [6,7] and have a false sense of security [8], which can lead to security negligence. McGill and Thompson [7] found that users tend to implement fewer security measures and have a lower perception of the severity of security threats and lower security self-efficacy on smartphones and tablets compared to their personal computers. In Clarke [9], over 20% of mobile device users were unaware of the security measures they were using. Breitinger et al. [10] found that smartphones are less secure compared to desktop computers.

Organizations, hence, have a stake in how employees manage their mobile devices. Mylonas et al. [11] found that employees tend to use the same device for work and personal purposes, escalating the threat to organizations' information security. The study also reported that users of smartphones did not enable or add security control, tended to disregard security when selecting and downloading applications, and were of the opinion that smartphone security software is not necessary. The reason behind the behavior and attitude was unclear. Experts have recommended the use of mobile device management (MDM) as an approach to restrict employees' mobile application installation rights and impose security practices. MDM is believed to reduce risks related to data security and intellectual property. However, there is a downside to MDM. The management of employees' personal devices puts additional strain on existing security infrastructures and threatens employees' privacy [12,13]. MDM also may limit and be contraindicative to the bring-your-own-devices (BYOD) culture implemented by organizations [14], restricting employees' freedom on the use of their personal devices for work purposes. According to Doargajudhur and Dell [15], BYOD culture positively impacts job satisfaction, job performance, and organizational commitment. The authors, nevertheless, did not include the influence of organizational control on the use of personal devices in their analysis.

Lima et al. [16] carried out an extensive analysis of MDM platforms from a security perspective and found that many MDM solutions are merely management solutions with some security features wrapped around specific applications, rendering these inadequate in monitoring the devices' contents, two-way communications patterns, or resource usage [17]. Therefore, information security related to the use of personal mobile devices is still very much dependent on usage behaviors. This study was, hence, carried out with the objective of investigating the factors influencing employees' security behaviors pertaining to the use of personal mobile devices. Set in Malaysia, this study strives to explain employees' decisions to protect their mobile devices by examining employees' cost–benefit consideration of mobile security practices and also the factors that influence this consideration. It is expected that the findings of this study shall provide insights that enable employers to better manage the use of mobile devices among employees.

2. Literature Review and Hypotheses Formulation

Employees' decision to practice good mobile security can be explained by the Rational Choice Theory (RTC). People are rational and pursue their self-interests based on their preferences [18] and choose to maximize their utility among the available options [19]. The theory states that an individual rationally decides based on cost–benefit considerations, and the chosen behavior will be the one with the best expected outcome [20]. Past studies have determined that cost–benefit considerations significantly influence employees' compliance with security policies [21], internet use policy [22], and employees' satisfaction with security practices [23]. It is, therefore, postulated that employees' decisions to implement mobile security measures depend on their cost–benefit consideration. Employees weigh between the cost of conforming to good practices and the expected benefits from the action as part of their decision process. Mobile security measures will be applied if the expected benefits of the action outweigh the perceived cost.

Nevertheless, individuals' preferences among the available choices can be selfish, altruistic, or influenced by social norms [19] and the organization they are in [20,22]. These elements form the personal and organizational context factors that influence employees' cost–benefit considerations. Personal factors include information security awareness and mobile usage behavior, while organizational factors are training, job characteristics, and monitoring [24–27]. The hypothesized relationships among these constructs are depicted in Figure 1. The next subsections discuss the cost–benefit consideration, personal aspects, and organizational context factors believed to affect mobile security practices among employees, as well as the available supports.

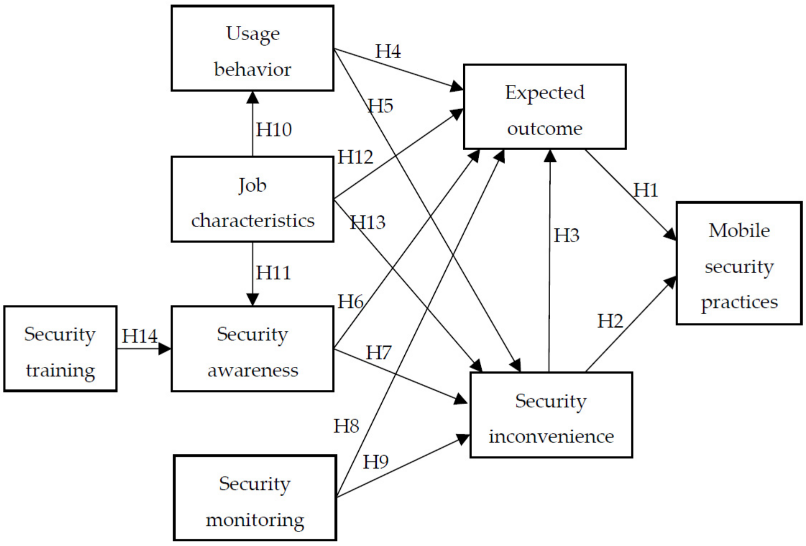

Figure 1. Hypothesized path model.

2.1. Cost–Benefit Consideration

Security measures are additional and usually non-automated actions that employees must intentionally perform in order to protect their mobile devices. We posited that these actions are conducted with the expectation that the actions will bring positive expected outcomes (benefits) within reasonable costs to the perpetrator. Expected outcome refers to the anticipated results or consequences of an action [28] and has been posited to determine behavior [21,29–32]. We believe that employees will take the necessary precaution to protect their mobile devices whenever they expect that such action will bring about positive outcomes, and the relevant hypothesis was constructed as below:

Hypothesis 1 (H1). *Expected outcome significantly affects mobile security practices.*

Past studies have shown that security measures are often viewed as inconvenient, effortful, and interrupting the achievement of assigned tasks. For example, in [33], the interviewed employees believed that security measures made it difficult for them to carry out their work. Security-related measures are generally viewed as bothersome and obstructive [34], constraining and inconvenient [35], and negatively impacting productivity [36], especially in the context of mobile devices. People tend to forsake their efforts when inconveniences are encountered [37–40]. The majority of respondents in [8] chose not to apply security measures to their mobile devices due to the complexity of the measures. Therefore, it was speculated that security inconvenience forms the cost of mobile security practices. The second hypothesis was formulated as follows:

Hypothesis 2 (H2). *Security inconvenience significantly affects mobile security practices.*

With regard to the use of mobile devices, we believe that the influence of inconveniences due to security measures is even more significant. This is because mobile devices are used for work purposes due to the convenience and utility provided. Nonetheless, the implementation of mobile security measures would instigate additional efforts on the part of the employees and reduce the expected utility. For example, a good security practice forbids the use of public networks. This limits the use of mobile devices when the employee does not have access to a secured network. Password-protected devices require employees to key in the password each time he or she needs to use the device, increasing the expected time to complete a task. Using a mobile device is no longer handy or useful if the employee has to grapple with various inconveniences of the security measures. Security inconvenience is thus believed to affect the expected outcome. This proposition is hypothesized below:

Hypothesis 3 (H3). *Security inconvenience significantly affects expected outcome.*

2.2. Personal Variables

Usage behavior and information security awareness are the two personal variables that were theorized to directly affect employees' cost–benefit consideration. Usage behavior of mobile devices provides first-hand experience to the employees and helps employees form judgments about security measures in a similar way asserted by [24]. Individuals form judgments about their behavior and the outcomes of the behavior based on their observations of the events that have occurred. The extent of various mobile applications or device usage leads employees to have direct knowledge of security issues and incidents [26] as well as a chance to learn through experience.

In Rhee et al. [25], for example, users who experienced a direct security breach as a result of mobile devices have been found to suffer a negative emotional state such as anxiety or stress. Such experience is an important source of information and influences one's behavior related to information security measures [27]. Employees who have used their mobile devices to store sensitive information would have formed more concrete judgments of the costs and benefits of mobile security measures. Stiakakis et al. [41] documented that users' concerns about mobile device security threats differed according to the frequency and variety of mobile services in use. We, therefore, posit that usage behavior significantly affects both expected outcome and security inconvenience. The relevant hypotheses are as follows:

Hypothesis 4 (H4). *Usage behavior significantly affects expected outcome.*

Hypothesis 5 (H5). *Usage behavior significantly affects security inconvenience.*

Bulgurcu et al. [21] have described security awareness as employees' understanding of information security and the relevant concerns. Information security awareness leads to employees' mindfulness of the significance of information security [42]. Thus far, information security awareness has been investigated in terms of its influence on users' perceptions and attitudes [21,43,44]. It could be deduced from Stanciu and Gheorghe [8] that security awareness affects users' decisions to implement security measures for their mobile devices.

However, Edwards [45], in his study of home users, found that information security awareness does not directly affect security behavior among users. Instead, security behavior was significantly affected by the perceived susceptibility to threats. Öğütçü et al. [46] noted that security awareness does not necessarily result in congruent behavior. It could be deduced from these studies that information security awareness may not directly affect behavior, but such awareness significantly influences users' judgment of the behavior. It is expected that information security awareness improves employees' cost–benefit consideration by helping employees to recognize possible outcomes of mobile security behavior and deal with the inconveniences of security measures. We, therefore, hypothesize that information security awareness affects the cost–benefit consideration of mobile security practices. Accordingly, the following hypotheses were constructed:

Hypothesis 6 (H6). *Information security awareness significantly affects expected outcome.*

Hypothesis 7 (H7). *Information security awareness significantly affects security inconvenience.*

2.3. Organizational Variables

Furnell and Rajendran [26] argued that organizational factors and job factors exert influence on employees' information security behavior. Organizational factors are (i) influences placed by the organization to promote and reinforce security issues to staff as well as (ii) work-related factors that shape the work norms of the employees. Based on the findings of past studies, we posited that three organizational variables are significant in determining employees' cost–benefit consideration of mobile security practices, namely, security monitoring, job characteristics, and training.

Security monitoring is implemented by organizations as a measure for information security [47,48] and to ensure compliance [49]. Security monitoring has been found to discourage information system abuse [49,50] and decrease employees' misbehavior [51]. Yan et al. [52] determined that information security monitoring positively influences organizations' security culture. We believe that information security monitoring enhances management's expectations of security behavior and shapes the information security norms of the organization. Whenever information security monitoring is truly executed, strong information security messages are conveyed to the employees. Hence, we theorize that such monitoring improves employees' mindfulness of security measures, which extends to the use of mobile devices. In an organization with a strong information security culture, the employees are believed to be more aware of the outcomes of security measures, and security measures become a habit rather than a chore. The following hypotheses were formed:

Hypothesis 8 (H8). *Information security monitoring significantly affects expected outcome.*

Hypothesis 9 (H9). *Information security monitoring significantly affects security inconvenience.*

The second organizational variable theorized to affect the cost–benefit consideration of mobile security practices is job characteristics. Past researchers have defined job characteristics as the qualities of a job that can motivate employees and have been proven to affect a wide range of behaviors [53]. The job characteristics theory [54] outlines five dimensions of job characteristics, namely, skill variety, task identity, task significance, autonomy, and feedback. The most relevant dimension related to this study is task significance—the degree to which the task affects others' life. A job tends to be more meaningful to employees whenever the job improves the well-being of others, whether in the organization or the external environment [54–56]. Employees are motivated by the perceived meaningfulness of the job, the responsibility of the job outcome, and the knowledge of the results [53].

In the context of the current study, we believe that the significance of a task is determined by the nature of information and data handled by the employees. Employees who handle confidential information and data would attach higher significance and responsibility to their tasks. Hence, job characteristics, within the context of this study, specifically refer to the extent of sensitive data and information handled by the employees. We posit that job characteristics significantly affect employees' usage behavior, information security awareness, expected outcome, and security inconvenience.

The employees who handle sensitive information would be more attentive to information security issues (awareness) and conscious about how they use their mobile devices as they are well aware of the information security threats that originate from mobile devices (usage behavior). The nature of tasks would also require employees to have higher expectations of security practices (expected outcome). Their job requirements would also require them to be more security conscious and to take security measures out of need rather than convenience. The related hypotheses are as below:

Hypothesis 10 (H10). *Job characteristic significantly affects usage behavior.*

Hypothesis 11 (H11). *Job characteristic significantly affects information security awareness.*

Hypothesis 12 (H12). *Job characteristic significantly affects expected outcome.*

Hypothesis 13 (H13). *Job characteristic significantly affects security inconvenience.*

The third organizational variable believed to be significant in relation to mobile security practices is security training. Security training forms organizational support, signals to employees the importance of such measures [27], and forms a strong system for controlling information security threats [34,57]. Past studies have shown that information security training is substantial in enhancing security awareness [42,57–59]. With information security training, employees gain information and knowledge about information security, including the importance of good security practices, ways to handle security issues, and threats to information security, among others. Thus, we posit that security training significantly enhances information security awareness by shaping the organization's security culture. The following hypothesis was developed.

Hypothesis 14 (H14). *Information security training significantly affects information security awareness.*

3. Research Methods

An online questionnaire survey was employed as the key data collection method for this study. The survey was conducted within a period of three months. The following subsections describe the research methods used in this study, including the sample, measurements, and analysis.

3.1. Sample

We have decided on telecommunication companies due to their core business, which places information security as the most critical need. Executive employees from these organizations were invited to take part in the survey via email communications to the organizations' contact persons. The contact person was requested to forward the invitation email to the executive employees. As employees' information was kept confidential by the organizations, we were not able to determine the response rate or implement specific selection criteria in the sampling process. Responses were received from 626 executives who were working in the target companies during the period of data collection, out of which 19 responses were discarded due to critical missing data or missing data for marker variables, namely, job position (executive or non-executive) and organization. The final sample consisted of 605 respondents.

Table 1 summarizes the demographic characteristics of the respondents. The majority of the respondents were in their 30 s (43.1%), followed by those in their 40 s (23.6%) and 20 s (22.8%). Male respondents made up 49.7% of the sample and female respondents 50.3%. Respondents were found to be well educated; more than 90% of the respondents received tertiary education. The demographic distribution was as expected since the target respondents were executive employees. The largest respondent group was from operations, production, and project management (30.9%), followed by the information systems and technology group (24.6%).

3.2. Measurements

A focus group discussion was conducted to develop the study's measurements. Representatives from the telecommunication industry, academics, and a local authority tasked with cybersecurity were the expert panels engaged in the discussion. The expert panels discussed issues related to information security, including mobile security. The panels also provided their expert evaluation of the research instrument. The panels agreed that the four behaviors selected either posed information security concerns or contributed to mobile information security. Ensuing from the discussion, a pilot study was conducted involving 84 employees from a selected organization. The research instrument was further refined.

The final measures and the response scale (shown in parentheses) used in the survey are as below, and the statements used in the questionnaire are in Appendix A:

1. Mobile security practice: Four items that gauged respondents' frequency of performing behaviors related to the use of public Wi-Fi, webmail, and the protection of mobile devices (1, never, to 6, very frequent).
2. Expected outcome: Respondents were requested to assess the possible outcome of each type of mobile security behavior (1, very negative, to 6, very positive).
3. Security inconvenience: Respondents were requested to gauge the functional impact of the selected mobile security behavior on their work (1, very easy, to 10, very troublesome).
4. Usage behavior: Three items related to the frequency (1, never, to 6, very frequent), expected benefits (1, very negative, to 6, very positive), and perceived utility of using mobile devices to store confidential information (1, very easy, to 10, very troublesome).
5. Job characteristic: Respondents were asked about the confidentiality level of data, information, and documents handled at work (1, not confidential at all, to 6, very confidential).
6. Security awareness: Four statements related to knowledge about information security, including actions to be taken, persons to contact, and relevant standards (1, strongly disagree, to 6, strongly agree).
7. Security monitoring: Four items related to the actions taken by the employing companies to oversee the use of information resources (1, never, to 6, very frequent).
8. Security training: Organization's emphasis on information security via training programs. Four statements were used (1, never, to 6, very frequent).
9. Security incident: Respondents were asked whether they had experienced security incidents before (yes, no, not sure).
10. Perceived risk: Respondents were to rate the likelihood of security incidents occurring within their department (1, very unlikely, to 6, very likely).

Table 1. Respondents' demographics.

		N *	**Percentage**
Age (in years):	age1: Below 30	138	22.8
	age2: 31–40	261	43.1
	age3: 41–50	143	23.6
	age4: 51–60	63	10.4
Gender:	gender0: Male	298	49.7
	gender1: Female	302	50.3
Academic qualification:	education1: Secondary school/certificate	8	1.3
	education2: Diploma	25	4.1
	education3: Bachelor's degree	467	77.4
	education4: Post-graduate	103	17.1
Job function:	jobfunction1: Sales and marketing	120	19.8
	jobfunction2: Accounting and finance	65	10.7
	jobfunction3: Operations, production, and project management	187	30.9
	jobfunction4: Information systems and technology	149	24.6
	jobfunction5: Facilities	15	2.5
	jobfunction6: Human resources and corporate communication	62	10.2
	jobfunction7: Security and risk management	8	1.3

* Variance in N is due to missing values.

3.3. Descriptive Statistics

Table 2 shows the descriptive statistics of the mobile security practices and security monitoring. We have classified the responses into three points, i.e., low (1, never, and 2, seldom), moderate (3, sometimes, and 4, quite frequent), and high (5, frequent, and 6, very frequent). Past literature has argued the importance of MDM in reducing information security risks that are related to the use of mobile devices. However, the implementation of MDM in organizations could still be very low. In this study, we were able to gauge the implementation of MDM in organizations by analyzing the level of security monitoring employed. As shown in Table 2, on average, employees rated each monitoring activity as “sometimes” (mean value of around 3.0). Based on further classification, security monitoring practices among the employing organizations could be said as low to moderate. Hence, it is also expected that MDM implementation among these organizations could also be at about the same level, if not lower.

Table 2. Descriptive statistics of mobile security practices.

Items	Mean	Low	Moderate	High
Mobile security practices *				
Use unofficial webmail to perform office duties such as sending sensitive information/documents (e.g., @yahoo.com; @hotmail.com).	1.762	82.8%	12.1%	5.1%
Access work-related emails via public networks such as Wi-Fi provided by a restaurant.	2.625	51.4%	37.3%	11.3%
Protect mobile devices such as handphones, tablets, and laptops with passwords, PINs, patterns, or other access control methods.	4.501	13.2%	27.7%	59.1%
Change your mobile devices’ passwords, PINs, patterns, or other access control methods at regular intervals.	3.374	28.6%	48.9%	22.7%
Security Monitoring *				
Conducts audit to detect the use of authorized software on its computers.	3.1	35.0%	45.7%	19.3%
Reviews logs of employee computing activities.	3.2	34.8%	46.4%	18.8%
Monitors employee computing activities.	3.4	27.1%	50.0%	22.9%
Monitors the content of employees’ email messages.	3.0	41.3%	39.8%	19.0%

* 6-point scale, ranging from 1 (never) to 6 (very frequent).

The most frequent security practice was protecting mobile devices with access control methods (mean = 4.501); 59.1% of the responses received were classified as high. Nevertheless, changing access credentials of mobile devices was less frequently performed (mean = 3.374), with the majority in the moderate category (48.9%). Almost 30% of the respondents either never or seldom changed their access credentials. Although respondents reported the use of unofficial webmail and public networks for work purposes as low (mean = 1.762 and 2.625, respectively), quite a number of respondents still did so. About 17% of the respondents reported the use of unofficial webmail for work purposes at moderate to high levels. Almost 50% of the respondents reported moderate to high use of public networks to access work-related emails.

In further analysis, we summed up the scores to form a continuous score for the variable mobile security practices, expected outcome, and security inconvenience. Negatively worded statements were reverse-scaled prior to computation. For mobile security practices, the composite scores varied from 10 at the lowest point and 24 at the maximum point. The scores for expected outcome ranged from 8 to 24 points, and the scores for security inconvenience ranged from 4 to 40. The scores indicate the extent of mobile security practices, expected outcome, and security inconvenience.

3.4. Factor Analysis

The data were factor-analyzed in order to classify items that were interrelated and to form composite variables to be tested in this study. We excluded the measures for mobile security practices, expected outcome, and security inconvenience from this analysis because the measures are not unidimensional and represent a range of behaviors related to mobile security. Five factors were generated from the analysis, and the supporting statistics showed acceptable results. The total variance explained was 76.911%, the Kaiser–Meyer–Oklin measure of sampling adequacy was acceptable at 0.860, and Bartlett test of sphericity was statistically significant (X^2 = 7535.00, d.f. = 153, p = 0.000). All factor loadings were above 0.70, and the items were loaded to each factor in accordance with the theorized dimensions. The Cronbach's alpha reliability statistic for each factor was also acceptable (above 0.60). Results of the factor analysis are depicted in Table 3. A composite variable representing each tested variable was then developed based on the factors by totaling the responses for each measurement item. The mean, standard deviation, skewness, and kurtosis statistics of the composite variables showed normal distribution and, thus, provided support for further analysis.

Table 3. Factor loadings and descriptive statistics for security training, security monitoring, security awareness, job characteristics, and usage behavior.

	Factor Loading	Cronbach's Alpha	Mean	Std. Dev.
Factor 1: Security monitoring		0.927	3.168	1.280
ST1	0.885			
ST2	0.862			
ST3	0.824			
ST4	0.814			
Factor 2: Security training		0.909	3.515	1.251
SM1	0.870			
SM2	0.815			
SM3	0.808			
SM4	0.769			
Factor 3: Security awareness		0.875	4.166	0.992
SA1	0.885			
SA2	0.852			
SA3	0.800			
SA4	0.783			
Factor 4: Job characteristic		0.941	4.406	1.015
JC1	0.945			
JC2	0.930			
JC3	0.928			
Factor 5: Usage behavior		0.631	4.407	1.423
UB1	0.783			
UB2	0.757			
UB3	0.737			

3.5. Analysis 1: Path Modeling

A path analysis, a structural equation modeling method, was conducted to test the hypothesized relationships among the multiple variables. This analysis was performed using SPSS Amos ver. 23. Path analysis enables a set of equations within a model to be computed concurrently and must only include measured variables. The chi-square goodness-of-fit test and other fit indices were used to establish the consistency between the observed model and the expected model. A comparative fit index (CFI) score larger than 0.95 [60], a goodness-of-fit statistic (GFI) larger than 0.90 [61], and root mean square approximation (RMSEA) of less than 0.06 [61,62] were used as indicators of a good model fit. Results of the path analysis showed a good fit (X^2 = 19.556; p = 0.050; X^2/df = 1.787; GFI = 0.992; CFI = 0.990; RMSEA = 0.036) and provided support for all hypotheses except H13. Twelve of the thirteen hypothesized paths were significant at the $p \leq 0.01$ level and were supported by the data. Table 4 shows the path coefficients of each hyphothesised relationships.

In Figure 2, solid lines signify significant path coefficients, and the dotted line indicates the non-significant path. The model predicted a 27% variation in mobile security practices (R^2 = 0.27), with security inconvenience as the strongest determinant (β = −0.37). Expected outcome (R^2 = 0.23) is significantly affected by security awareness (β = 0.12), security monitoring (β = −0.11), usage behavior (β = 0.12), and security inconvenience (β = −0.39). Security inconvenience is mainly predicted by security awareness (β = 0.20), followed by usage behavior (β = −0.16) and security monitoring (β = −0.09).

Table 4. Path coefficients.

	Hypothesized Paths	β	S.E.	C.R.		Std. β
H1:	Expected outcome ⟶ Mobile security practices	0.229	0.036	6.425	*	0.246
H2:	Security inconvenience ⟶ Mobile security practices	−0.173	0.018	−9.567	*	−0.366
H3:	Security inconvenience ⟶ Expected outcome	−0.198	0.019	−10.276	*	−0.392
H4:	Usage behavior ⟶ Expected outcome	0.090	0.027	3.336	*	0.122
H5:	Usage behavior ⟶ Security inconvenience	−0.239	0.057	−4.148	*	−0.164
H6:	Security awareness ⟶ Expected outcome	0.306	0.141	3.730	*	0.096
H7:	Security awareness ⟶ Security inconvenience	−1.199	0.298	−4.720	*	−0.190
H8:	Security monitoring ⟶ Expected outcome	−0.278	0.097	−3.242	*	−0.112
H9:	Security monitoring ⟶ Security inconvenience	−0.444	0.207	−2.515	*	−0.091
H10:	Job characteristic ⟶ Usage behavior	0.403	0.171	2.362	*	0.096
H11:	Job characteristic ⟶ Security awareness	0.144	0.032	4.042	*	0.147
H12:	Job characteristic ⟶ Expected outcome	0.295	0.116	2.297	*	0.085
H13:	Job characteristic ⟶ Security inconvenience	0.250	0.249	1.163		0.041
H14:	Security training ⟶ Security awareness	0.307	0.029	10.368	*	0.348

* Path is significant at the 0.01 level.

3.6. Analysis 2: Ordinal Regression Analysis

Ordinal logistic regression analysis was conducted to determine the influence of demographic and work-related variables on mobile security practice to supplement the path analysis results and provide more insight into employees' mobile security practices. Demographic and work-related variables are categorical in nature and could not be adequately examined using path analysis. The dependent variable, mobile security practice, was first transformed into six ordinal categories in order to facilitate the analysis. The transformation involved calculating the percentiles of the responses and reclassification of the responses into six categories, namely, 1—Never, 2—Seldom, 3—Sometimes, 4—Quite frequent, 5—Frequent, and 6—Very frequent. The continuous score was used for calculating the percentiles in the 17th, 30th, 50th, 66th, 83th, and 100th percentiles. Corresponding values received from the percentiles were used in categorizing the responses. Table 5 presents the data distribution of mobile security practice after the transformation. Average values of each respondent for work-related independent variables, past security experience, and perceived risk were calculated to be used in the analysis. The data distribution of work-related independent variables is depicted in Table 6.

Ordinal logistic regression analysis that included likelihood ratio tests, parameter estimates, and tests of parallel lines were performed on the data. The likelihood ratio tests in Table 7 show the significance of each of the independent variables. Four of the independent variables have *p*-values that are less than 0.05, indicating there is a significant relationship between the variables and the dependent variables, namely, "Gender, "Job function", "Past security experience", and "Perceived risk".

Looking further into parameter estimates for these four independent variables in Table 8, the odds of mobile security practice for females (gender1) are 0.616 times lower than the odds of mobile security practice for males (reference group: gender0). Next, the odds of mobile security practice for someone whose work function was security and risk management (jobfunction7) are 4.246 times higher than the odds of mobile security practice for someone who works in sales and marketing (reference group: jobfunction1). Moreover, the odds of mobile security practice for someone who has experienced prior security incidents (incident1) are 0.665 times lower than the odds of mobile security practice for someone who has no known past security incident (reference group: incident0). Additionally, the odds of mobile security practice for someone who perceived that the risk of information security is quite likely (reference group: risk4) are 0.478 times lower than the odds of mobile security practice for someone who perceived the risk to be very unlikely (reference group: risk1).

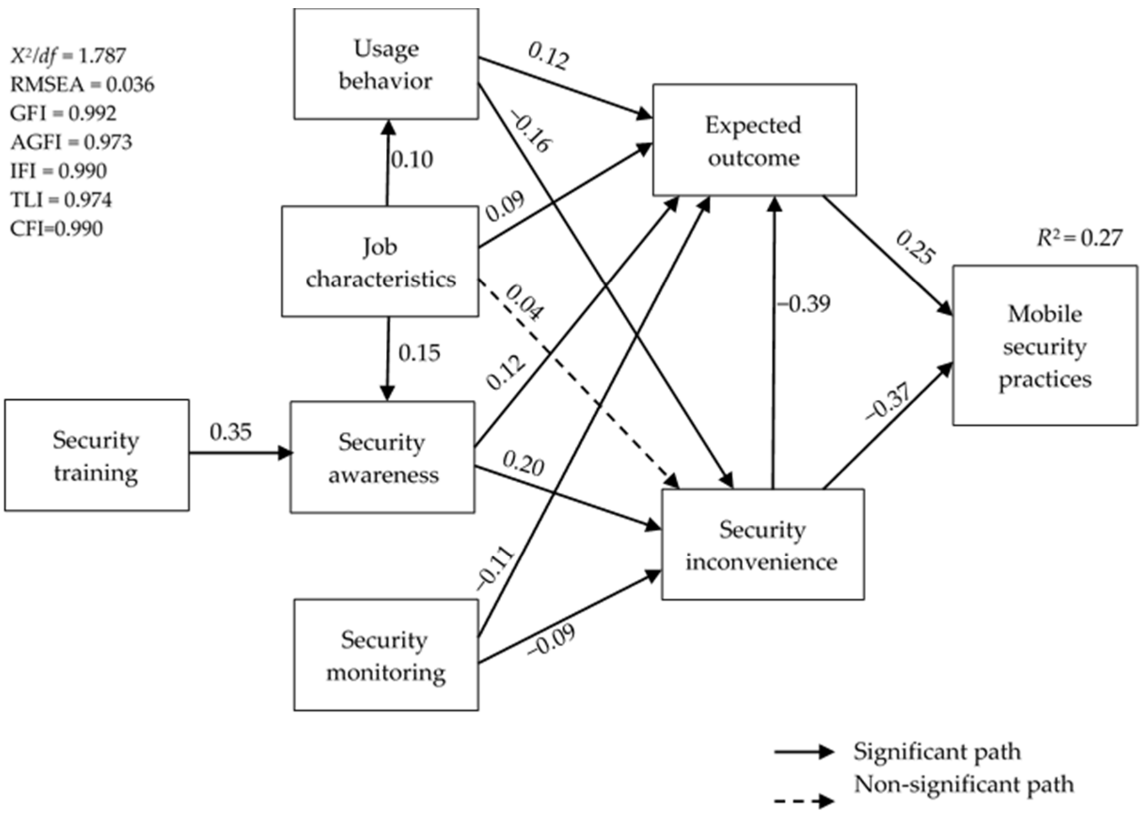

Figure 2. Observed path model.

Table 5. Data distribution of mobile security practice after transformation.

		N	Percentage
Mobile security practice:	Never	158	26.1
	Seldom	64	10.6
	Sometimes	85	14.0
	Quite frequent	144	23.8
	Frequent	52	8.6
	Very frequent	102	16.9

Table 6. Data distribution of work-related variables.

		N	Percentage
Past security experience:	incident0: No known past security incident	400	66.1
	incident1: Has prior security incident	205	33.9
Perceived risk:	risk1: Very unlikely	60	9.9
	risk2: Unlikely	117	19.3
	risk3: Quite unlikely	170	28.1
	risk4: Quite likely	157	26.0
	risk5: Likely	76	12.6
	risk6: Very likely	25	4.1

Table 7. Omnibus likelihood ratio tests.

Predictors	χ^2	*df*	*p*
Gender	10.31	1	0.001
Age	2.33	3	0.507
Education	2.13	3	0.546
Job function	13.17	6	0.040
Past security experience	6.71	1	0.010
Perceived risk	24.07	5	<0.001

Table 8. Parameter estimates.

						95% Confidence Interval	
Predictor	**Estimate**	**SE**	**Z**	***p***	**Odds Ratio**	**Lower**	**Upper**
Gender:							
gender1–gender0	−0.4846	0.151	−3.2013	0.001	0.616	0.457	0.828
Age:							
age2–age1	0.1340	0.192	0.6991	0.485	1.143	0.785	1.666
age3–age1	0.3229	0.218	1.4789	0.139	1.381	0.901	2.121
age4–age1	0.2371	0.283	0.8379	0.402	1.268	0.727	2.209
Education:							
education2–education1	0.7973	0.751	1.0612	0.289	2.220	0.500	9.801
education3–education1	0.3422	0.672	0.5091	0.611	1.408	0.367	5.339
education4–education1	0.2820	0.692	0.4078	0.683	1.326	0.334	5.217
Job function:							
jobfunction2–jobfunction1	−0.3450	0.281	−1.2278	0.220	0.708	0.407	1.227
jobfunction3–jobfunction1	−0.0553	0.213	−0.2594	0.795	0.946	0.623	1.437
jobfunction4–jobfunction1	0.3679	0.221	1.6617	0.097	1.445	0.936	2.232
jobfunction5–jobfunction1	0.0401	0.478	0.0839	0.933	1.041	0.404	2.667
jobfunction6–jobfunction1	0.0671	0.292	0.2296	0.818	1.069	0.602	1.896
jobfunction7–jobfunction1	1.4460	0.638	2.2679	0.023	4.246	1.195	15.193
Past security experience:							
incident1–incident0	−0.4082	0.158	−2.5867	0.010	0.665	0.488	0.905
Perceived risk:							
risk2–risk1	0.2918	0.289	1.0109	0.312	1.339	0.761	2.362
risk3–risk1	−0.2100	0.274	−0.7667	0.443	0.811	0.474	1.388
risk4–risk1	−0.7391	0.279	−2.6494	0.008	0.478	0.276	0.825
risk5–risk1	−0.5012	0.318	−1.5778	0.115	0.606	0.325	1.129
risk6–risk1	−0.1187	0.454	−0.2615	0.794	0.888	0.363	2.163

Ordinal logistic regression assumes that the effects of independent variables are consistent across different thresholds, which is also known as the proportional odds assumption. For instance, it assumes that the coefficients that describe the relationship between the lowest versus all higher categories of the dependent variable are the same as the coefficients that describe the relationship between the second-lowest category and all higher categories. A test of parallel lines was carried out to test this assumption, and the result is presented in Table 9. The null hypothesis states that the lines of the model are parallel. As shown in Table 9, the test result of the ordinal logistic regression model is non-significant as the significance value is 0.729. Thus, the null hypothesis is accepted, which is interpreted as the assumption of consistency effects of independent variables is fulfilled.

Table 9. Test of parallel lines [a].

Model	−2 Log Likelihood	Chi-Square	*df*	Sig.
Null hypothesis	1639.435			
General	1571.328 [b]	68.107 [c]	76	0.729

The null hypothesis states that the location parameters (slope coefficients) are the same across response categories; [a] = Link function: Logit; [b] = the log-likelihood value cannot be further increased after maximum number of step-halving; [c] = the chi-square statistic is computed based on the log-likelihood value of the last iteration of the general model. The validity of the test is uncertain.

4. Discussion and Conclusions

This study was conducted with the aim of deliberating mobile security practices among employees and examining the possible antecedents. In accordance with the rational choice theory, we hypothesized that employees would implement mobile security practices after considering the costs (security inconvenience) and benefits (expected outcome) of the practice while being conditioned by the organizational environment (information security monitoring, job characteristics, information security training) and personal characteristics.

Security inconveniences are an aspect of information security that should receive more attention from researchers. The theoretical contribution of this study can be observed in terms of specifying and operationalizing the costs and benefits consideration of mobile security practices. Models that explain the behavioral response towards security implementation should incorporate elements of inconvenience—either towards the use of the security measures itself or inconvenience in terms of achieving work targets. The findings of this study also highlight the potential of integrating rational choice theory with other behavioral theories such as the theory of reasoned action (TRA), the technology acceptance model (TAM), or the unified theory of acceptance and use of technology (UTAUT).

Security measures are not without costs to both the organizations and the employees alike. While costs to the organizations are easier to determine, the costs borne by the employees are less apparent. This study has analyzed security inconvenience as a form of costs incurred by employees, and this cost was found to be significant in determining their security-related behaviors. The implementation of MDM by organizations, therefore, should consider this cost to the employees, especially when BYOD culture is applied. When faced with inconveniences, people either choose to avoid the course of action or find ways to circumvent the inconveniences. In the context of organizations, this is counter-productive and may even compromise information security controls. This is a significant implication that must be considered by MDM developers.

MDM is to provide central control over policies, applications, and additional functions to mobile device usage. To a certain extent, effective MDM could complement BYOD in the workplace. It is considered a balanced and enhanced security measure for organizations by ensuring control over confidential data while allowing the convenience of using user-owned devices connecting to the system resources owned by organizations. From the organizational perspective, efforts need to be made to reduce the anxiety of user privacy issues as well as inconvenience concerns over the use of MDM solutions in future work.

Anticipated benefits (expected outcomes) were found to positively affect mobile security practices (H1). Security inconvenience significantly and negatively affects mobile security practices (H2) and the expected outcome (H1). The results show support for the rational choice theory and highlight the importance of considering security inconvenience as a cost to information security measures. Inconveniences due to security measures also reduce the anticipated benefits of security efforts. The adoption of mobile devices in the workplace should strike a balance between security and usability. To accomplish this, the employee should allow the company's security experts to assess the security of their devices, and, at the same time, the employees should be allowed to evaluate the device's usability with the implementation of mobile security measures. As such, security measures and security policies should be designed with convenience in mind.

Personal variables, namely, usage behavior, were found to significantly affect the expected outcome (H4) and security inconvenience (H5). Usage behavior was examined based on employees' experience in using mobile devices to store confidential data in terms of frequency, security utility, and benefits. It was predicted that usage behavior forms employees' first-hand experience on security issues, and the results show support for this notion. Higher usage behavior could be associated with positive expected outcomes and reduced security inconvenience. Hence, for organizations keen to implement a bring-your-own-device (BYOD) campaign, it would be beneficial if employees are first entrusted with low levels of mobile access; the access can be increased as they become more experienced users. The evolution of BYOD will be inclusive and refined according to employer and employee expectations.

Security awareness, another personal variable examined, was found to negatively affect security inconvenience (H7) and positively affect expected outcomes (H6). Higher security awareness is, therefore, associated with lower security inconvenience and higher expected outcomes. Security awareness thus favorably affects employees' cost–benefit considerations towards implementing good mobile security measures. This indicates the significance of enhancing security awareness among employees. As employees are the most vulnerable connection within the security defense mechanism, the employer should create the right awareness program to educate employees about good security practices and, thus, limit the possibility of security breaches. Implementing security awareness will ensure desirable security behavior and compliance among the employees in using mobile devices for their official tasks and responsibility.

Three organizational variables were tested in this study, namely, security monitoring, job characteristics, and security training. Security monitoring was determined to negatively affect both expected outcome (H8) and security inconvenience (H9). It could be deduced from the results that security monitoring hampers the anticipated benefits of mobile devices, although it somehow reduces security inconvenience, perhaps due to increased awareness or familiarity among the employees. Hence, organizations, through security monitoring, should have a better understanding of employees' ways of handling mobile devices and its security practices while leveraging the usefulness of mobile devices. Organizations should consider implementing applications for the verification and enforcement of mobile security policies, such as those deliberated by Armando et al. [63], de las Cuevas et al. [64], and Dong et al. [65]. This is an area where application developers should exert more focus since the existing technologies to oversee BYOD implementation are still in infancy and are perhaps even less understood among the employees [66,67].

Job characteristics, in terms of handling sensitive information and data, were found to significantly affect usage behavior (H10), security awareness (H11), and expected outcome (H12). The findings provide evidence that employees who are entrusted with the care of confidential data are more likely to be more experienced in handling such data and, thus, more confident, have higher security awareness, and anticipate more positive outcomes from mobile security practices. This study, however, could not establish any relationship between job characteristics and security inconvenience (H13).

Finally, security training was found to significantly affect security awareness (H14). This finding showed evidence of security training in enhancing security awareness. Thus, conducting security training, especially on mobile security practices, would be beneficial whenever organizations have the intention to implement a BYOD program. Security training nurtures and develops a culture of security in the organization, leading to awareness of potential security breaches and the relevant security measures. It is, thus, recommended to train the employee on how to properly manage sensitive data of mobile devices, ways to respond to any security breaches, and the understanding of BYOD policy.

This study found that employees' cost–benefit consideration of mobile security practices is strongly affected by the information security culture of the organization. The culture is affected by various factors, among which include the training conducted, organizational policies and enforcement, and responsibilities assigned. It is imperative that organizations develop a culture that prioritizes ethical tone [68], information security, and policy compliance via appropriate encouragements, enforcement, and sanctions. Based on the findings in Cho and Ip [66], it could be deduced that compliance efforts that are linked to job security could be worth considering. We also support the recommendations forwarded by Zahadat et al. [69] that organizations should consider the elements of people, policy management, and technology in BYOD program implementation, which is applicable to mobile security practice.

Ordinal logistic regression was implemented to explore the relationship between the demographic and work-related data of the employees and their mobile security practice. The analysis result revealed that the variables "Gender", "Job function", "Past security experience", and "Perceived risk" are significantly associated with the mobile security practice of the employees. Analyses of parameter estimates have shown that being female (gender1), prior security incidents (incident1), and perceiving information security incidents as quite likely (risk4) negatively influence mobile security practice, while the job function of security and risk management (jobfunction7) has a positive influence on mobile security practice. From the test of parallel lines, the proportional odds assumption was satisfied for the ordinal logistic regression model, which means the coefficients of independent variables are the same across all different categories of the dependent variable.

5. Limitations and Future Works

The research output may be limited due to potential social desirability bias, whereby respondents tried to portray themselves in a good light, which could have affected the results. Response bias, such as over-reporting positive behavior or under-reporting negative or undesirable behavior, will provide the tendency toward untruthful and biased results of the survey. The results are also limited to telecommunication companies, and, thus, the application of the findings to other industries should be carried out with caution. To further validate the results, we recommend this study be replicated in other industries where private and confidential information is vastly collected and retained, such as the financial industry and education and healthcare sectors.

Moreover, the scope of research was restricted to the rational choice theory, with a focus on personal behavior and organizational factors. Future studies should, therefore, consider other factors such as management styles, industry, and work environment. In general, the finding of this study shows that job characteristics are not significant in relation to perceived security inconvenience. It is, therefore, proposed that more extensive research be done on mobile device security to explore this construct further in the future, in particular in relation to MDM. In this work, we attempt to gauge the implementation of MDM in organizations by analyzing the level of security monitoring employed. However, we did not collect much information on MDM in the study, and we did not measure the practice of MDM specifically. As such, there is insufficient evidence to conclude any findings on MDM from this paper. Other than the issue of security inconveniences, studies on MDM should further investigate behavioral implications over user privacy. Privacy concerns have always been found to suppress the expected benefits of BYOD programs, [70] and related compliance costs have been found to be a strong deterrent to compliance [71]. This is an area that remains to be addressed substantially.

Author Contributions: Conceptualization, Z.A., T.S.O., T.H.L. and M.N.; methodology, Z.A. and T.S.O.; software: Z.A. and Y.W.G.; formal analysis: Z.A., Y.W.G. and T.S.O.; validation: T.H.L., M.N. and T.S.O.; data curation, Z.A. and Y.W.G.; writing—original draft preparation, Z.A.; writing—review and editing, T.S.O., Y.W.G., T.H.L. and M.N.; funding acquisition: Z.A. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS/2/2013/SS05/MMU/02/12).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Mobile security practice:	
How frequent do you perform the following? 1, never, to 6, very frequent	
SP1	Use unofficial webmail to perform office duties such as sending sensitive information/documents (e.g., @yahoo.com; @hotmail.com).
SP2	Protect mobile devices such as hand phones, tablets and laptops either with passwords, PINs, patterns, or other access control methods.
SP3	Access work-related emails via public networks such as Wi-Fi provided by a restaurant.
SP4	Change your mobile devices' passwords, PINs, patterns, or other access control methods as regular intervals.
Expected outcome:	
If the following tasks were performed in your organization, what is the possible outcome? 1, highly negative to 6 highly positive	
OE1	Use unofficial webmail to perform office duties such as sending sensitive information/documents (e.g., @yahoo.com; @hotmail.com).
OE2	Protect mobile devices such as hand phones, tablets and laptops either with passwords, PINs, patterns, or other access control methods.
OE3	Access work-related emails via public networks such as Wi-Fi provided by a restaurant.
OE4	Change your mobile devices' passwords, PINs, patterns, or other access control methods as regular intervals.
Security inconvenience:	
By performing these tasks, your work will become: 1, very easy to 10, very troublesome	
PE1	Use unofficial webmail to perform office duties such as sending sensitive information/documents (e.g., @yahoo.com; @hotmail.com).
PE2	Protect mobile devices such as hand phones, tablets and laptops either with passwords, PINs, patterns, or other access control methods.
PE3	Access work-related emails via public networks such as Wi-Fi provided by a restaurant.
PE4	Change your mobile devices' passwords, PINs, patterns, or other access control methods as regular intervals.
Usage behavior:	
UB1	How frequent do you store confidential information in personal mobile devices such as hand phones, tablets and laptops. *1, never, to 6, very frequent*
UB2	By storing confidential information in personal mobile devices such as hand phones, tablets and laptops the possible outcome is *1, highly negative to 6 highly positive*
UB3	By storing confidential information in personal mobile devices such as hand phones, tablets and laptops, your work will become *1, very easy to 10, very troublesome*
Job characteristic:	
1, Not sensitive at all to 6, Highly sensitive	
JC1	You usually handle documents that are . . .
JC2	You usually handle information that are . . .
JC3	You usually handle data that are . . .
Security awareness:	
Rate your agreement to the following statements. 1, Strongly disagree to 6, Strongly agree	
SA1	You know who to contact in the event of information security breach.
SA2	You know what to do in the event of information security breach.
SA3	You know the standard operating procedures in handling private and confidential information.
SA4	You know who the security officers in your organization are.
Security monitoring:	
How frequent does your organization conduct the following activities? 1, Never to 6, Very frequent	

SM1	Conducts audit to detect the use of authorised software on its computers.
SM2	Reviews logs of employee computing activities.
SM3	Monitors employee computing activities.
SM4	Monitors the content of employees' e-mail messages.
Security training:	
How frequent does your organization conduct the following activities? 1, Never to 6, Very frequent	
ST1	Briefs employees on the consequences of modifying computerised data in an unauthorised way.
ST2	Communicates the importance of confidentially and privacy of data.
ST3	Provides employees with education on computer software copyright laws.
ST4	Educates employees on their computer security responsibilities.

References

1. Cisco BYOD Insights 2013 (2013, March). Available online: http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&SWTHEMEID=12949 (accessed on 15 February 2019).
2. Morrow, B. BYOD security challenges: Control and protect your most sensitive data. *Netw. Secur.* **2012**, *2012*, 5–8. [CrossRef]
3. Jones, B.H.; Heinrichs, L.R. Do business students practice smartphone security? *J. Comput. Inf. Syst.* **2012**, *53*, 22–30.
4. Mobile Devices Still Unsecured in the Workplace. Available online: https://www.eweek.com/mobile/mobile-devices-still-unsecured-in-the-workplace/ (accessed on 15 February 2019).
5. Hayes, D.; Cappa, F.; Le-Khac, N.A. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. *Digit. Bus.* **2020**, *1*, 100001. [CrossRef]
6. Imgraben, J.; Engelbrecht, A.; Choo, K.R. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behav. Inf. Technol.* **2014**, *33*, 1347–1360. [CrossRef]
7. McGill, T.; Thompson, N. Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behav. Inf. Technol.* **2017**, *36*, 1111–1124. [CrossRef]
8. Stanciu, V.; Gheorghe, M. Facing the mobile revolution: A Romanian insight. *Account. Manag. Inf. Syst.* **2019**, *18*, 101–118. [CrossRef]
9. Clarke, N.; Symes, J.; Saevanee, H.; Furnell, S. Awareness of Mobile Device Security: A Survey of User's Attitudes. *Int. J. Mob. Comput. Multimedia Commun.* **2016**, *7*, 15–31.
10. Breitinger, F.; Tully-Doyle, R.; Hassenfeldt, C. A survey on smartphone user's security choices, awareness and education. *Comput. Secur.* **2020**, *88*, 101647. [CrossRef]
11. Mylonas, A.; Kastania, A.; Gritzalis, D. Delegate the smartphone user? Security awareness in smartphone plat-forms. *Comput. Secur.* **2013**, *34*, 47–66. [CrossRef]
12. Yamin, M.M.; Katt, B. Mobile device management (MDM) technologies, issues and challenges. ICCSP'19. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 143–147.
13. Garba, A.B.; Armarego, J.; Murray, D.; Kenworthy, W. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Int. J. Inf. Secur. Priv.* **2015**, *11*, 38–54. [CrossRef]
14. Barthwal, D. Mobile Device Management (MDM) in Organizations. 2016. Available online: https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations (accessed on 15 February 2019).
15. Doargajudhur, M.S.; Dell, P. Impact of BYOD on organizational commitment: An empirical investigation. *Inf. Technol. People* **2018**, *32*, 246–268. [CrossRef]
16. Lima, A.; Borges, P.; Sousa, B.; Simões, P.; Cruz, T. An Introduction to Mobile Device Security. In *Mobile Apps Engineering: Design, Development, Security, and Testing*; Mostefaoui, G.K., Tariq, F., Eds.; CPC Press, Taylor & Francis Group: Boca Raton, FL, USA, 2019.
17. Lima, A.; Rosa, L.; Cruz, T.; Simões, P. A Security Monitoring Framework for Mobile Devices. *Electronics* **2020**, *9*, 1197. [CrossRef]
18. Jeong-Yeon, L.; Younghwa, L.; Wadhwa, P. Conference Paper Sharing Among Academicians: Calculative and Normative Aspects of Rational Choice. *Acad. Manag. Learn. Educ.* **2010**, *9*, 204–224. [CrossRef]
19. Moscati, I.; Tubaro, P. Becker random behavior and the as-if defense of rational choice theory in demand analysis. *J. Econ. Methodol.* **2011**, *18*, 107–128. [CrossRef]
20. Paternoster, R.; Simpson, S. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law Soc. Rev.* **1996**, *30*, 549–584. [CrossRef]
21. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information security policy compliance: An empirical student of rationality-based beliefs and information security awareness. *MIS Q.* **2010**, *34*, 523–548. [CrossRef]
22. Li, H.; Zhang, J.; Sarathy, R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis. Support Syst.* **2010**, *48*, 635–645. [CrossRef]
23. Montesdioca, G.Z.; Maçada, A.G. Measuring user satisfaction with information security practices. *Comput. Secur.* **2015**, *48*, 267–280. [CrossRef]
24. Bandura, A. *Self-Efficacy: The Exercise of Control*; W.H. Freeman: New York, NY, USA, 1997.

25. Rhee, H.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Comput. Secur.* **2009**, *28*, 816–826. [CrossRef]
26. Furnell, S.; Rajendran, A. Understanding the influences on information security behavior. *Comput. Fraud. Secur.* **2012**, *2012*, 12–15.
27. Tu, Z.; Turel, O.; Yuan, Y.; Archer, N. Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Inf. Manag.* **2015**, *52*, 506–517. [CrossRef]
28. McAlister, A.L.; Perry, C.L.; Parcel, G.S. How individuals, environments, and health behaviors interact: Social cognitive theory. In *Health Behavior and Health Education: Theory, Research, and Practice*, 4th ed.; Glanz, K., Rimmer, B.K., Viswanath, K., Eds.; Jossey-Bass: San Francisco, CA, USA, 2008; pp. 169–188.
29. Ng, B.Y.; Kankanhalli, A.; Xu, Y. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
30. Jose, S.; Babu, D. A study on the role of performance and image outcome expectations on innovative behavior in the workplace. In Proceedings of the ISPIM Conferences, Manchester, UK, 17–20 June 2012; pp. 1–33.
31. Williams, C.K.; Wynn, D.; Madupalli, R.; Karahanna, E.; Duncan, B.K. Explaining Users' Security Behaviors with the Security Belief Model. *J. Organ. End User Comput.* **2014**, *26*, 23–46. [CrossRef]
32. Seyeon, C.; Goo Hyeok, C.; Jing, D. *Employees' Attributions to Innovation and Implementation Behaviors*; Academy of Management: Briarcliff Manor, NY, USA, 2015; p. 1.
33. Albrechtsen, E. A qualitative study of users' view on information security. *Comput. Secur.* **2007**, *26*, 276–289. [CrossRef]
34. Hovav, A.; Putri, F.F. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive Mob. Comput.* **2016**, *32*, 35–49. [CrossRef]
35. Posey, C.; Roberts, T.L.; Lowry, P.B.; Hightower, R.T. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inf. Manag.* **2014**, *51*, 551–567. [CrossRef]
36. Beautement, A.; Sasse, A. The economics of user effort in information security. *Comput. Fraud. Secur.* **2009**, *2009*, 8–12. [CrossRef]
37. Rajamma, R.K.; Paswan, A.K.; Hossain, M.M. Why do shoppers abandon shopping cart? Perceived waiting time, risk, and transaction inconvenience. *J. Prod. Brand. Manag.* **2009**, *18*, 188–197. [CrossRef]
38. Cheng, Y.; Liu, K. Evaluating bicycle-transit users' perceptions of intermodal inconvenience. *Transp. Res. Part A Policy Pract.* **2012**, *46*, 1690–1706. [CrossRef]
39. Liang, D.; Ma, Z.; Qi, L. Service quality and customer switching behavior in China's mobile phone service sector. *J. Bus. Res.* **2013**, *66*, 1161–1167. [CrossRef]
40. Barbarossa, C.; Pelsmacker, P. Positive and negative antecedents of purchasing eco-friendly products: A comparison between green and non-green consumers. *J. Bus. Ethics* **2016**, *134*, 229–247. [CrossRef]
41. Stiakakis, E.; Georgiadis, C.; Andronoudi, A. Users' perceptions about mobile security breaches. *Inf. Syst. e-Bus. Manag.* **2016**, *14*, 857–882. [CrossRef]
42. Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H. The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Comput. Educ.* **2009**, *52*, 92–100. [CrossRef]
43. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behavior formation in organizations. *Comput. Secur.* **2015**, *53*, 65–78. [CrossRef]
44. Hanus, B.; Wu, Y. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Inf. Syst. Manag.* **2016**, *33*, 2–16. [CrossRef]
45. Edwards, K. Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale-Davie, FL, USA, December 2015.
46. Öğütçü, G.; Testik, Ö.M.; Chouseinoglou, O. Analysis of personal information security behavior and awareness. *Comput. Secur.* **2016**, *56*, 83–93. [CrossRef]
47. Hoffman, W.M.; Hartman, L.P.; Rowe, M. You've got mail and the boss knows: A survey by the center for business ethics of companies' email and internet monitoring. *Bus. Soc. Rev.* **2003**, *108*, 285–307. [CrossRef]
48. Samaranayake, V.; Gamage, C. Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *Telemat. Inform.* **2012**, *29*, 233–244. [CrossRef]
49. D'Arcy, J.; Hovav, A.; Galletta, D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Inf. Syst. Res.* **2009**, *20*, 79–98. [CrossRef]
50. Trinkle, B.S.; Crossler, R.E.; Warkentin, M. I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *J. Inf. Syst.* **2014**, *28*, 307–327. [CrossRef]
51. Zoghbi-Manrique-de-Lara, P. Predicting nonlinear effects of monitoring and punishment on employee deviance: The role of procedural justice. *Eur. Manag. J.* **2011**, *29*, 272–282. [CrossRef]
52. Yan, C.; Ramamurthy, K.; Kuang-Wei, W. Impacts of comprehensive information security programs on information security culture. *J. Comput. Inf. Syst.* **2015**, *55*, 11–19.
53. Rahim, A.R.A.; Shabudin, A.; Nasurdin, A.M. Effects of Job Characteristics on Counterproductive Work Behavior Among Production Employees: Malaysian Experience. *Int. J. Bus. Dev. Stud.* **2012**, *4*, 123–145.
54. Hackman, J.R.; Oldham, G.R. Motivation through the design of work: Test of a theory. *Organ. Behav. Hum. Perform.* **1976**, *16*, 250–279. [CrossRef]

55. Shamir, B.; Salomon, I. Work-at-home and the quality of working life. *Acad. Manag. Rev.* **1985**, *10*, 455–464. [CrossRef]
56. Grant, A.M. The significance of task significance: Job performance effects, relational mechanisms, and boundary conditions. *J. Appl. Psychol.* **2008**, *93*, 108–124. [CrossRef]
57. Mete Eminağaoğlu, M.; Uçar, E.; Eren, Ş. The positive outcomes of information security awareness training in companies: A case study. *Inf. Secur. Tech. Rep.* **2009**, *14*, 223–229. [CrossRef]
58. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of Awareness and Training on Cyber Security. *J. Internet Commer.* **2010**, *9*, 23–41. [CrossRef]
59. Da Veiga, A.; Martins, N. Information Security Culture: A Comparative Analysis of Four Assessments. *Proc. Eur. Conf. Inf. Manag. Eval.* **2014**, *8*, 49–57.
60. Bentler, P.M. Comparative Fit Indexes in Structural Models. *Psychol. Bull* **1990**, *107*, 238–246. [CrossRef]
61. Hooper, D.; Coughlan, J.; Mullen, M.R. Structural equation modeling: Guidelines for determining model fit. *Electron. J. Bus. Res. Methods* **2008**, *6*, 53–60.
62. Steiger, J.H. Understanding the limitations of global fit in structural equation modelling. *Pers. Individ. Differ.* **2007**, *42*, 893–898. [CrossRef]
63. Armando, A.; Costa, G.; Merlo, A.; Verderame, L. Formal modeling and automatic enforcement of Bring Your Own Device policies. *Int. J. Inf. Secur.* **2015**, *14*, 123–140. [CrossRef]
64. De las Cuevas, P.; Mora, A.M.; Merelo, J.J.; Castillo, P.A.; García-Sánchez, P.; Fernández-Ares, A. Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Comput. Commun.* **2015**, *68*, 83–95. [CrossRef]
65. Dong, Y.; Mao, J.; Guan, H.; Li, J.; Chen, Y. A Virtualization Solution for BYOD With Dynamic Platform Context Switching. *IEEE Micro* **2015**, *35*, 34–43. [CrossRef]
66. Cho, V.; Ip, W.H. A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterp. Inf. Syst.* **2018**, *12*, 659–673. [CrossRef]
67. Veljkovic, I.; Budree, A. Development of Bring-Your-Own-Device Risk Management Model: A Case Study from a South African Organization. *Electron. J. Inf. Syst. Eval.* **2019**, *22*, 1–14.
68. Crossler, R.E.; Long, J.H.; Loraas, T.M.; Trinkle, B.S. The Impact of Moral Intensity and Ethical Tone Consistency on Policy Compliance. *J. Inf. Syst.* **2017**, *31*, 49–64. [CrossRef]
69. Zahadat, N.; Blessner, P.; Blackburn, T.; Olson, B.A. BYOD security engineering: A framework and its analysis. *Comput. Secur.* **2015**, *55*, 81–99. [CrossRef]
70. Lee, J.; Warkentin, M.; Crossler, R.E.; Otondo, R.F. Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *J. Comput. Inf. Syst.* **2017**, *57*, 309–318. [CrossRef]
71. Crossler, R.E.; Long, J.H.; Loraas, T.M.; Trinkle, B.S. Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *J. Inf. Syst.* **2014**, *28*, 209–226. [CrossRef]