Journal of Universal Computer Science, vol. 23, no. 12 (2017), 1113-1131
submitted: 23/2/17, accepted: 25/7/17, appeared: 28/12/17 © J.UCS

Developing a BYOD Scale to Measure the Readiness Level: Validity and Reliability Analyses

Murat Topaloglu[1]
(Trakya University, Kesan Yusuf Çapraz School of Applied Sciences, Edirne, Turkey
murattopaloglu@trakya.edu.tr)

Dilek Kırar
(Trakya University, Kesan Yusuf Çapraz School of Applied Sciences, Edirne, Turkey
d_krr@hotmail.com)

Abstract: The BYOD programme is a trend that aims to provide companies and workers with the next generation of security methods and flexible business models. These have been developed recently as a result of technological developments, especially in smart devices.
Individuals from the "Y generation", who are also called the millennials, have a significant influence on shaping the present and future technology. Y generation employees want to use their own devices, including their own personal applications. Allowing employees to use their own devices does not mean that you will lose anything or have no control. For this reason, the BYOD policy, when implemented at a good level, significantly increases business performance and increases the productivity with the benefits provided by mobility. The BYOD tendency, which is difficult to avoid, increases the productivity of employees and the flexibility of the company in the eyes of the employees, by letting them use their own devices in the business environment. Moreover, it reflects positively on the employees' morale, with a subsequent increase in company loyalty.
The aim of this study is to evaluate the validity and reliability analyses done during the development of the scale which aims to measure the effects of BYOD on workers and to assess its security components, benefits, applicability and sustainability. Our goal is to revise the previous research done and present objective values and findings obtained from the analyses. These values were based on the demographic information and the answers given by participants about to what extent BYOD is known and legal, its vulnerabilities in infrastructure and data security, the way it affects workers' perceptions individually and in general, and the benefits it provides.
SPSS 20 program was used for descriptive statistics, exploratory factor analysis (EFA), confirmatory factor analysis (CFA), item analyses and correlation coefficients.

Keywords: BYOD, IT Policy, Scale Development and Validation, Business Management
Categories: A.1, C.0, H.4.1, J.4, K.4

1 Introduction

The rapid developments in technology have led to a great many changes in various fields. Technological devices used for business are of the utmost importance. The increasing number of devices and applications that employers have to provide for

[1] Corresponding author

their employees also affects the cost and performance of the employees. The trend of IT adaptation leads business people to different strategies which allow and increase the use of IT devices at work [Lüker et al., 2016]. Although the presence of the workers is required in the workplace, employees tend to complain about the time they spend in the office as a result of the rapid developments in the Internet and mobile technologies.

BYOD helps companies free up their employees to bring their electronic devices pursuant to the company policy which enables them to use the device they like and are familiar with for corporate purposes [Herand & Çalışır, 2014; Ryan et al., 2013]. BYOD is a trend whose aim is to ease the adoption of modern business models. It makes the adaptation process easier by allowing the employees to use their own devices in the workplace. Remote management and teleworking have been gaining importance day by day in the modern business models. Employees can access intranets via corporate services and communication networks by using their own devices. Companies invest in the systems that provide the employees with access to the corporate networks at any time and anywhere in order to increase the mobility. Bringing your own device technology that emerged as a solution to decrease costs will be used by many more companies in the upcoming years [Yılmaz, 2014].

1.1 The Advantages of BYOD

Corporate firms, public institutions, universities, private institutions and even non-governmental organisations that work voluntarily, support BYOD.

Today, devices like smart phones and tablet computers have become a part of organisations to form a stronger IT structure within the companies [Harris et al., 2012]. When managed well, IT adaptation which has commonly been used among the employees/devices is very likely to increase customer satisfaction and reduce the IT cost [Giddens & Tripp, 2014; Niehaves et al., 2012]. IT adaptation has become a trend drawing the attention of the many IT leaders in which the use of technological devices at work is launched by the employees who are IT users [Putri & Hovav, 2014; Weiß & Leimeister, 2012]. Harris et al., 2012 stated that the employees often perceive Information Technology as "more powerful, easier to use, faster attainment and more fun"

Worldwide companies seek to find solutions with teleworking days and special rights. Giant companies like Microsoft allow their employees to work at home on a day they choose. From a technical aspect, BYOD is designed to support smart phones, tablets and laptops.

1.2 BYOD Productivity

The use and knowledge of technology among the employees is quite dynamic as it changes day by day. Employees seem to force their employers to adapt to new technologies [Andriole, 2012]. They also demand the integration of the current IT conditions and proper policies into their business process. Business enterprises have adopted various approaches for the IT adaptation process [Vandelannoitte, L., 2015]. The use of IT resources for personal affairs is a common trend observed in the IT adaptation process [; Burt, 2011; Harris et al., 2012; Vogel et al., 2010; Weiß & Leimeister, 2012]. Taking these trends into account, companies generally allow the

personal use of IT resources within the organisation. Business enterprises try to produce new strategies and BYOD policies including those dealing with these kinds of problems and to encourage employees to bring their own devices to work [Andel, 2011; Burt, 2011; Threlkeld, S., 2011]. Company policies are an important guide for IT adaptation. Risk analysis and individualisation are some of the important factors affecting the BYOD process.

Although the employees have the right to choose which user-based IT devices to buy and use [Harris et al., 2012], company policies for BYOD, the use of devices at work, security, data privacy and cyber loafing is still debated and researched [Andel, 2011; Burt, 2011; Chou et al., 2008]. Negative results like the decrease in productivity are present [Bock & Ho, 2009] in literature and recommendations are made to prevent these kind of behaviours [Hu et al., 2011; Lee & Lee, 2002; Shepherd & Klein, 2012; Ugrin & Pearson, 2008; Zhang et al., 2006).

On the other hand, the IT adaptation process may result in an increase in the backup costs of IT devices [Bernnat et al., 2010]. When the personal devices are integrated into the organisation, the number of measures also increases. However, some studies show that productivity increases as the use of BYOD helps to increase the level of employee satisfaction [Threlkeld, S., 2011].

Studies indicate that BYOD needs to be promoted and the savings from the devices will help the companies [Andel, 2011; Threlkeld, S., 2011]. The devices used for business purposes at work and for personal affairs will still be defined as BYOD. BYOD is very productive as long as it follows the organisational rules and takes the necessary deterrent measures. To sum up, the borders of work-daily life cycle with respect to the newly developed devices have been disappearing with the adaptation process.

1.3 The Flexibility of BYOD

Employees' IT habits and preferences for device use should be investigated for compatibility [Lüker et al., 2016]. The traditional authoritarian strategy model in IT management in business enterprises emphasises the use of IT devices and some technical issues [György et al., 2012]. Business enterprises have defined three different IT user strategies to deal with the new trend [Harris et al., 2012]. The Laissez-faire strategy states that the purchase and use of IT devices should be limited to only a small extent. Middle Ground strategies claim that user-centreed IT devices that can work on different levels should be purchased while Authoritarian Strategy underlines that each category of technology should have some standards with tight controls [Harris et al., 2012]. On the other hand, the productivity of these three strategies is still dubious [Moyer, 2013]. The level of productivity can also be influenced by some factors like employees and companies [Morrow, 2012; Tokuyoshi, 2013]. These factors can vary from the security concerns of the companies and the employees' wish to work in a more comfortable and less stressful place. If the companies apply compelling policies to employees, then the IT integration process will become more difficult. Harris et al., 2012 state that although one out of every three companies follows tight control strategies, adaptation seems to be of importance. Company management can identify the BYOD strategies by clarifying their expectations of the IT adaptation and the employees can follow them. Besides, by allowing the employees to choose their own IT devices and applications (Choose Your Own

Device – CYOD) it is possible to increase employee satisfaction and overall productivity [Ortbach et al., 2013].

1.4 The Security of BYOD

Mobile devices like smartphones now also have the power to support many applications that are supported by computers [Couture, 2010]. One of the most important problems with the devices used at work is the potential security flaws which are not mentioned in the organisational policies [Harris et al., 2012]. Despite the useful and practical features of mobile devices, their physical connections with various networks and servers render them vulnerable to the security holes. The unauthorised use of the user devices can be named as "shadow IT" fear. "Shadow IT" can be defined as the unauthorised use of the devices by a user without the permission of the authorised IT department responsible for the hardware, software or the organisational ecosystem [Silic & Back, 2014]. The unauthorised use of IT devices often causes trouble between the management and IT [Behrens, 2009]. Besides, user-centred innovations, that are not compatible with the corporal system, result in security threats [Furnell et al., 2006; György et al., 2012; Niehaves et al., 2012]. Because the number of companies legalising the adaptation process by allowing the use of the devices within the organisation [Botha et al., 2009; Fitzgerald, 2009; Harris et al., 2012; Niehaves et al., 2012; Vandelannoitte, L., 2015] keeps growing, so do the security concerns but certain guidelines can be formed for the technical borders. When the employees' behaviours conflict with organisational IT standards, adaptation problems may occur [Ortbach et al., 2013]. Even though the IT determines which devices will be used by the employees, the BYOD strategies will be determined by the employees' choices. If the organisation has difficulties in determining the devices in IT units, it can lead to information security problems [Chen & Nath, 2011; Manz and Stewart, 1997; Walton, 1999] and loss of reputation [French et al., 2014; Morrow, 2012].

1.5 The Role of BYOD in Education

BYOD is quite popular in companies, educational institutions and common spaces. The wide use of mobile devices also promotes the development of BYOD strategies [Bengisoy, 2017; Kocakoyun & Bicen, 2017]. Those strategies go against the use of traditional desktops and policies. The use of BYOD has made the traditional computer labs. less popular and encourages students to bring their own devices [Ozdamli & Tavukcu, 2016; Uzunboylu & Tugun, 2016]. BYOD practices around the world have been a popular subject in recent literature. BYOD has been regarded as a prerequisite of e-learning in education.

2 Related Works

The study [Chou et al., 2017] investigated the effect of BYOD (bring your own device) on student language learning. The research scenario is the use of smartphones through an application in the classroom environment. With the long-term use of the BYOD approach, students were more productive than with the classical approach.

This approach has provided more consistent results for the sustainability of learning. The students' second language learning experiences, especially with the BYOD approach, have improved their motivation and knowledge. The results of the study indicate that schools and teachers need to explore creative ways to integrate traditional approaches and the BYOD approach.

The work [Lüker et al., 2016] aimed to measure the IT adaptation in two higher education institutions using two different strategies (Laissez-faire and Middle-ground) and the policy-related attitudes of the employees and their abilities to work with policy-compliant devices. Based on these two theories, the data were obtained from interviews with thirty-six employees working on procedural justice theory, transaction cost theory and mixed methods. The findings paradoxically show that, although the middle-ground strategies are comprehended at a high level, the satisfaction of the policies were quite low. The shareholders at an organisational level (e.g., CEOs and IT managers) and the department-level employees participated in semi-structured interviews. It provides qualitative and quantitative evidence related to the different policies and attitudes and behaviours of the employees.

The study [Hovav & and Putri, 2016] examines the company employees' intentions to comply with the BYOD security policies. Reaction, protecting the motivation and organisational justice theories were used to create a research model. The findings of the study reveal that employees who understand the company's security policies will positively influence their intention to comply with them. On the other hand, the understanding of freedom that exists in employees affects the harmonisation process negatively. There is a dual effect of the security perception enhancement programme: this programme increases the response efficacy in a positive direction and the response cost in a negative direction. The presence of an IT support team for BYOD increases employee efficacy and perceived justice.

Ortbach et al., 2013 developed a theoretical model for the IT consumer behaviour based on a quantitative analysis and theory planned behaviour. The data were collected through an online survey and analysed with the SPSS program. They developed a model to explain the individualisation process in the Information System and the IT-user trends relationship, and to test the theoretical behaviours of the IT users. It showed that the individualisation behaviour cannot be determined based on several factors. It requires a complicated set of factors to determine the behaviour. The model in general showed that it is important for the individuals not to cross the lines of other individuals and the possible results of the use of technology.

Schalow et al., 2013 probed the employees' use of the IT resources and media for corporal and personal purposes with different forms from a broad perspective. Fourteen employees from five different companies were interviewed. After a comprehensive review of social sciences literature, a theory was established to help to discover the blurred borders of the work and personal lives. The findings of the study showed that employees had different attitudes towards the work/life turbidity and that mobile IT has an accelerating role in the process. A conceptual model was formed for the conditions and results. The results also showed that, while some employees advocated the use of personal devices at work, some did not.

Harris et al., 2012 investigated the adaptation process of the organisation and the resulting conflicts. Information Technologies aim to maximise the advantages of the use of IT resources and minimise the security risks. This study focused on the

adaptation process of the organisations and the minimisation of the risks at work during the process. Management strategies for IT Consumerism were defined and the Laissez-Faire and Authoritarian Strategies were addressed.

Sarker et al., 2012 found that the productivity in the organisation increased when the employees made use of mobile technologies. However, there are concerns that the use of mobile devices can have a negative effect on the work/life balance of employees. This study investigated the undesirable effects on WLB and presented framework and management strategy plans for WLB management. They also stated that WLB perceptions differed by work life and personal life style and that these perceptions are sustainable. Moreover, some participants thought that, although work and personal life overlap at some points, they never merge. The results of the study showed that the active use of mobile technologies brought a new understanding, including different points of view, of the relationship between work and personal life. The management strategies designated to deal with the work/life balance problems stemming from the use of mobile technologies need to be in accordance with the team-level and individual-level perceptions. The productivity should be taken to a maximum level by choosing the right strategies for the employees to have a practical work/life balance at a desired level.

Although BYOD is a relatively new subject, there is already some research available. It includes subjects such as the analysis of the next generation technological approaches [Carideo et al., 2013; Güneş, 2014], next generation business models [Aydın, 2014; Phillips, 2012; Sarıkoz, 2015], mobile applications [Huang, 2013; Pitichat, 2013], data management [Ruggiero & Foote, 2011], flexible business models [Emery, 2012] and policies that provide data security infrastructure [Belletati. 2014; Garcia 2013; Kocamustafaoğulları, 2013; Pitichat 2013]

3 Methodology

3.1. Scale Development Process

The BYOD scale was developed and validated using the scale development and validation procedures suggested by MacKenzie et al., 2011. Actually, to avoid obtaining any extreme values giving artificial findings, it was necessary to process data cleaning, missing data imputation and data preparation. Originally, MacKenzie et al., 2011 summarised ten steps to develop a scale. However, for the purpose of this study, we only employed five steps since this paper addresses the initial stage of scale validation. The steps employed in this study are; (1) conceptualisation, (2) item generation and refinement (3) pilot-testing and scale purification (4) data collection (5) reliability and validation analysis.

3.1.1 Step-1: Conceptualisation

The aim of this study is to evaluate the validity, reliability and confirmatory factor analyses done during the development of the scale which aims to measure the effects of BYOD on workers and assess its security components, efficiency, benefits, applicability and sustainability. The validation and reliability study of the scale was carried out for that purpose. This study includes the effects of mobile infrastructure

and BYOD on employees' personal and business lives. It aims to clarify the adaptation of BYOD by companies and employees and the perceptions of BYOD.

Thus, we started with the conceptualisation process by determining the dimensions that can explain the latent variable. This step needs to be conducted before the development of a scale because a clear link between the generated items and their domain needs to be established. Before the development of the items in the scale, the studies on BYOD were reviewed and the employees and IT managers in various companies were interviewed.

3.1.2 Step-2: Scale Items Generation & Refinement

Before the construction of the scale, a literature review was undertaken to examine the emergence of BYOD, the features it has, the use of BYOD and the other measurable dimensions of it. In addition, data were collected from a heterogeneous small size sample in order to represent the target group related to the subject investigated and the individuals in the study group were expected to express their feelings, ideas and attitudes towards the subject. An opinion form with open ended questions was prepared and given to fifteen employees. According to Tavşancıl, 2010, when analysed systematically, the elements mentioned in the compositions can give clues to the expressions to be written. So, the data obtained from the compositions were used to create the item pool. Fifty-four statements that were thought to be related to BYOD were identified after the data analysis.

The statements, including technological, individual or social subjects with negative and positive attitudes, were distributed evenly. The items in the scale will be developed in 5-Likert type.

3.1.3 Step-3: Pilot-testing & Scale Purification

After the 54-item testing scale was developed, it was given to a group chosen randomly from the companies. Next, a group of employees, apart from the sample, were asked to correct the possible misunderstandings in the statements and troubled items were excluded. After purification of all the scales, an outline form was prepared including forty-two items. The outline of the scale was reviewed by the experts for content validity and some statements were altered for its final form which included forty-two items. Based on the statistical results of our study; additional modifications were made. Purification is a procedure conducted to remove the items which do not contribute to the internal consistency of a particular construct. Finally, the scale was determined to have twenty items after factor analyses were done.

Descriptive statistics for the total scores of the items are presented below. Those values show that the data to be analysed fits the normal distribution. In order to test the construct validity and define the factor groups, exploratory factor analysis was used. The aim of the factor analysis is to form a group by gathering the items that measure the same factor and entitle each factor group with respect to the item properties within the group [Karasar, 2013].

The construct validity of *scale* was checked with the exploratory factor analysis and total item correlations. Principal components analysis was used for the data analysis. The total score for each participant ranges from 28 to 99. According to the

results, the range is 71. The mean, the median and the standard deviation were calculated as 95 and 9.49021, respectively. The skewness and the Kurtosis were found to be -.751 and 2.459, respectively. According to the bulk data results, the distribution seems normal. Thus, it can be said that higher scores seem to indicate that participants have more positive attitudes while interpreting the scale.

Before the factor analysis, Kaiser-Meyer-Olkin (KMO) and Bartlett's test for sphericity results should be obtained. A certain amount of correlation between the variables is also required for the factor analysis [Şencan, 2005]. Bartlett's test of sphericity shows whether the relation between the variables is adequate. If the p value of the Barlett test is below 0.05 significance level, it means that the relationship between the variables is sufficient for factor analysis.

According to the test results, the KMO value was found to be 0.807 and this value was found acceptable as it has normal distribution in the context of the study. The values above 0.80 in KMO are thought to be perfect for factor analyses [Büyüköztürk, 2009; Hutcheson & Sofronio, 1999; Leech et al., 2005; Namlu & Odabasi, 2007; Tavşancıl, 2010]. The Bartlett test done for the study was found to be meaningful (χ^2= 2154.229; $p < 0.005$).

That the Bartlett's test done for the study was found to be meaningful shows that data were collected from a multivariable normal distribution. As the items with low factor load values were not included in the scale, there was no need to repeat the calculations for factorisation. If the factor load of an item is below 0.50 or the difference between the factor loads of more than one item is less than 0.10, it is recommended to exclude the item(s) from the scale [Büyüköztürk, 2009; Çokluk et al., 2010]. While Kaiser-Meyer-Olkin (KMO) measures the conformity of the whole question set with the factor analysis in general, Measures of Sampling Adequacy (MSA) value measures the conformity of each and every question with the factor analysis. If the MSA value of a question is below 0.50, that question should be excluded from the question analysis. None of the values in the diagonal of Anti-image Correlation matrix are below 0.50. According to Kline, 1994, the factor load values represent the relationship between the items and the factors.

According to Child, 2006, determining factors are based on the assumption of the correlation between the scores producing linear relations. Although all of the linear combinations cannot be tested for normality, an evaluation can be made with the normality, kurtosis and skewness coefficients [Büyüköztürk, 2009]. After the "BYOD Scale" was determined, Cronbach's Alfa, (α) internal consistency coefficients for the scale and sub-dimensions were calculated. The reason for using Cronbach's Alfa (α) for reliability is that the scale is Likert type and that it could be administered only once.

The distribution properties of the scale scores were reviewed before the item analysis was done. Descriptive and procedural statistics techniques were used for this review. Cronbach's Alfa (α) was used in order to determine the reliability of the assessment instrument. The factors with α values less than 0.50 were excluded from the scale. The internal consistency coefficient for the scale was 0.828.

3.1.4 Step-4: Data Collection

Data were collected from experts employed in Turkey during 2016 and 2017. Among three hundred and twenty-two participants, twenty-one of them were eliminated

because of the missing data and data obtained from the rest of the three hundred and one individuals were used for the data analysis. The number of individuals in the study group in terms of sample size was at least five times the number of items recommended for the use of factor analysis [Child, 2006; Tavşancıl, 2010]. %60.8 (183) of the participants were males while %39.2 of them (118) were females %80.1 of the participants ranged between 22-40 in terms of age.

3.2. Scale Validation

3.2.1 Step-5: Exploratory Factor Analysis and Validation

Component factor loads for twenty items were calculated for the distinctive properties of the items in the scale. The items in the scale are shown in Table 1 and the factor load ranges are between 0.578 and 0.836. In order to assign the questions to factors, factor loads for each question should be checked and a question should be assigned to the related factor for which it gets the highest score.

There have to be more than one hundred and twenty observations for a factor load of 0.50 to be meaningful [Alpar, 2011]. By looking at this value, the items below 0.50 are recommended to be excluded, not that the exclusion of the items is a conventional criterion. Thus, there are no items with a low common factor variance. Rotated factor analysis results were used for the determination of item factor load values. Assuming that there is no relation between the factors, Varimax vertical rotation technique was used. According to the analysis results, factor loads of the items range between 0.578 and 0.836. According to the results, twenty items analysed fell under five factors whose eigenvalues were above 1.00.

The results obtained for the factor rotation are as follows; %14.116, %13.633, %13.171, %11.933 and %8.773 for the first, second, third, fourth and fifth dimension variance quantities, respectively. The estimated variance quantity (average variance explained) represented by the five-factor scale was calculated as %61.626.

It is safe to say that the scale would have five factors. The first one is "the sustainability of BYOD" with four items, the second one is "the security components of BYOD" with five items, the third one is "the advantages of BYOD" with four items, the fourth one is "the effects of BYOD on users" with four items and the last one is "the preliminary preparation for BYOD" with three items.

Items and factors	Mean	SD	Factor Loading	Item-to-total Correlation
24. Companies BYOD will remain incapable of tracking lost/stolen devices.	2.98	.980	.836	.693
26. Companies BYOD will fall behind in terms of the use of personal devices and applications.	3.06	1.028	.834	.715
25. Companies BYOD will fall short in terms of management/support.	3.13	.978	.823	.712
27. Companies BYOD will fall short in terms of cost.	3.07	.981	.778	.614
Factor I: "the sustainability of BYOD", $\alpha = .846$				

20. In order to protect the BYOD related measuring instruments, corporate networks and the data, location tracking software should be installed to the personal devices.	3.54	1.047	.786	.598
19. BYOD and security measuring instruments, private virtual networks and virtual desktops should be used to protect the corporate networks and data.	3.56	.920	.771	.591
21. BYOD and security measuring instruments, employers should be restricted to downloading unsecure applications to protect the corporate networks and data.	3.46	1.084	.752	.559
18. BYOD and security measuring instruments, the number of devices on the network should be restricted to protect the corporate networks and data.	3.55	.984	.607	.546
17. BYOD and security measuring instruments, it is necessary to make sure that the devices and applications that employees use are up-to-date to protect the corporate networks and data.	3.78	.965	.598	.542
Factor II: "the security components of BYOD", α = .788				
15. BYOD programme will be beneficial to employers and employees.	3.62	.940	.813	.652
14. The use of personal devices and applications in the workplace will be beneficial to the employers.	3.74	1.027	.759	.632
12. The use of personal devices and applications for business purposes will be beneficial to the employees.	3.36	.975	.746	.629
13. The use of personal devices and applications for business purposes will improve the performance of the employees.	3.58	.985	.713	.578
Factor III: "the advantages of BYOD", α = .807				
41. BYOD increases the number of smart devices used in business.	3.76	.994	.808	.619
37. BYOD/A puts more responsibility on employees as a result of the use of personal devices for work.	3.77	.890	.710	.506
40. BYOD makes the character analysis of the employers easier for companies.	3.43	.969	.670	.513
42. BYOD helps employees adapt to workplace environment more easily as they are used to their own devices and applications.	3.66	.986	.616	.501
Factor IV: "the effects of BYOD on users", α = .741				

8. The personal devices and applications are sufficient for BYOD.	3.14	1.007	.814	.540
9. The infrastructure provided for your personal devices is sufficient for high-toned uninterrupted connection and access to data.	3.07	.930	.732	.473
11. BYOD will be the most common implementation in our country in the short term.	3.23	.919	.578	.395
Factor V: "preliminary preparation for BYOD", α = .656				

Table 1: Results of Scale Purification

The mean, standard deviation, factor loading, common factor variance of the items and item-to-total correlation results are shown in Table 1. The rotated factor load values indicate that all the items are reasonably valid.

Cronbach's alpha reliability coefficient of each factor was calculated in the following way: for the first factor α = 0.846, second factor α = 0.788, third factor α = 0.807, fourth factor α = 0.741, fifth factor α = 0.656. Cronbach's Alfa (α) factor based reliability coefficients indicated that all of the factors had high reliability. According to our findings, the whole scale and the reliability coefficient of the sub-dimensions are over 0.60, therefore proving that our scale is indeed reliable [Sipahi et al., 2010].

3.2.2 Item–factor correlation analysis

At the last stage of the reliability test, the Pearson Correlation Coefficient was examined in order to clarify the relation between the factors and the relation of the factors to the scale total score. To do this, the total score of each item in each factor was found and total scores for the 20-item scale were recalculated with respect to its final form. The data obtained from the analysis are shown in Table-2.

Dimension	Sustainability	Security	Advantages	Effects on Users	Preliminary Preparation
Sustainability	**1**				
Security components	**,146***	**1**			
Advantages	**-,061**	**,239****	**1**		
Effects on users	**,137***	**,446****	**,375****	**1**	
Preliminary preparation	**,023**	**,262****	**,505****	**,366****	**1**
*. Correlation is significant at the 0.05 level (2-tailed).					
**. Correlation is significant at the 0.01 level (2-tailed).					

Table 2: Correlation Matrix of Dimension

The correlation analysis showed that some factors have a low and medium level of relationship with the total scale scores at $p<0.01$ level. The correlation analysis showed that some factors do not have a meaningful relationship with the total scale scores at $p<0.01$ level, which means that there is no linear relationship between the two factors.

3.2.3 Confirmatory Factor Analysis

Confirmatory factor analysis is a type of structural equation model that helps to determine the relationship between the observed and latent variables and is considered to be an important part of adaptation studies of scales. The analysis results obtained using the SPSS-Amos program are presented in Table-3.

Fit Measures	Good Fit	Acceptable Fit	Model Value
χ^2/df	χ^2/df < 3	3 < χ^2/df < 5	2.061
GFI	.95 ≤ GFI ≤ 1	.90 < GFI < .95	.903
RMSEA	0 < RMSEA < .05	.05 < RMSEA < .08	.059
TLI	.95 ≤ TLI ≤ 1	.90 < TLI < .95	.900
CFI	.95 ≤ CFI ≤ 1	.90 < CFI < .95	.918

Table 3: Fit indices for Confirmatory Factor Analysis

Confirmatory factor analysis results for standardised results are shown in Figure 1.

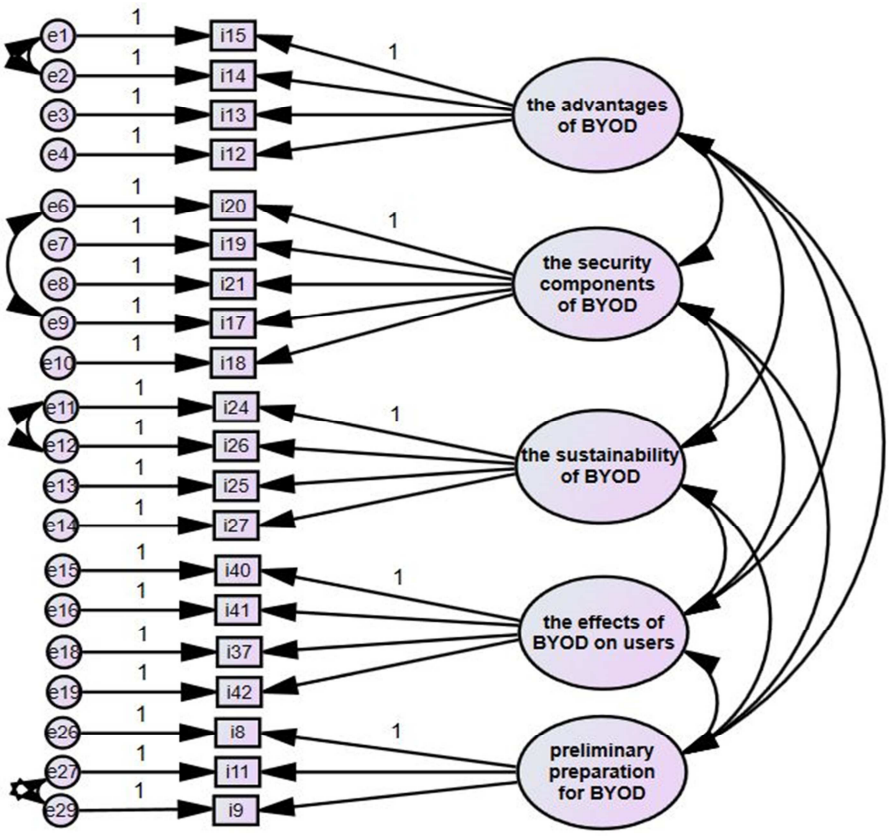

Figure 1: CFA with Standardized Results

4 Discussion

Flexible working used to be regarded as a way of bringing about a balance between personal and business life, reducing travel expenses and saving time on behalf of the employees only. However, flexible working strategies not only increase the productivity of the employees but also allow people to connect with each other anywhere via videos, thus making companies primary beneficiaries, too. Recent developments like corporate mobility and the cloud bring along new opportunities. Flexible working applications, which are increasingly used in departments related to Computer Technologies, will find a wider use in other fields, too. The concept of BYOD (Bring Your Own Device) is likely to turn into BYOA (Bring Your Own Application) and people will probably want to use the applications they are familiar with as BYOD becomes more popular. As it becomes possible to access information anywhere with an increasing number of employees noticing this fact, more investments will be made in solutions in order to assess success more effectively.

Global companies, with younger employee profiles and who specialise in technology, believe that it is necessary to grasp the meaning of BYOD and adopt it. Thus, it is not possible to ignore the rise of the BYOD trend. On the other hand, the companies who support the use of BYOD need to take some precautions.

First of all, the personal devices to be used should be compatible with the central devices of the company that provide the service to make sure that they are available for communication on standard protocols. Secondly, there should be the assurance of communication media and data security. Apart from that, the culture of the company should also be welcoming towards this application. Companies provide their employees with the flexibility of teleworking by using cutting edge technology within the scope of various adaptation processes. Security is still a critical issue to be worked on in almost all cases. No matter what devices are used, whether the ones provided by the company or the ones that are owned by the employees, what matters most is to raise awareness and responsibility in users. How the companies deal with security policies and convey them to the users plays an important role.

5 Conclusion

At this point, where BYOD is concerned, companies have to set a clear policy on what their employees are allowed and not allowed to do.

Institutions must take the impact of the Y Generation when taking IT decisions into account. The fact that the Y Generation becomes widespread and becomes a totally dominant generation has an increasing influence on the determination of IT strategies. For this reason, it is necessary first to take the IT strategies that will meet the demands and needs of the Y generation into consideration.

When IT offers applications and services that meet the security requirements but ignore the user experience, they will prefer to find their own solutions.

In situations where a large number of employees are accessing the internet from their own devices, network security becomes more critical for the enterprises. When businesses lose control over these devices, it is inevitable that company resources become more vulnerable to viruses and malicious programs.

Defining user groups for employees, using multiple SSID and tunnel protocol options to protect company resources and prevent data breaches, and implementing Unified Threat Management solutions are also effective ways to protect networks. Considering these explanations, the importance of the study emerges.

In this study, an assessment instrument whose reliability and validity were proven was developed to measure the attitudes of the employees of some companies operating in Turkey towards the use of BYOD. According to the validity and reliability test results, the scale including twenty items under five factors and was thought to be fit for the purpose of measuring the attitudes of the employees towards the use of BYOD. The factors in the scale were named "the sustainability of BYOD", "the security components of BYOD", "the advantages of BYOD", "the effects of BYOD on users" and "the preliminary preparation for BYOD". The variance rate explained by the five factors in the scale was %61.626. Factor loads of the items varied between 0.578 and 0.836. In the light of the item analysis results based on the internal consistency (t-Test), it was concluded that the scale items had distinctive properties in terms of measuring the intended characteristics. Internal consistency coefficient for the whole scale was found to be 0.828.

"Developing the BYOD Scale to Measure Readiness Level", which was developed for this study, is thought to be a guiding and supportive resource for future research whose intended population is employees working in companies. The aforementioned scale was developed to assess and evaluate the attitudes towards the use of BYOD in companies and educational institutions.

References

[Alpar 2011] Alpar, R.: Uygulamalı çok değişkenli istatistiksel yöntemler, (3rd ed.), 2011, Ankara: Detay Yayıncılık.

[Andel 2011] Andel, T.: Bring your phone to work?, Material Handling & Logistics, 2011, 66 (12), 26.

[Andriole 2012] Andriole, S.J.: "Managing Technology in a 2.0 World", IT Pro (January / February), 2012, 50–57.

[Aydın 2014] Aydın, Ö.: Analysis of erp softwares, sap software and developing a sap integrated retailing software, MSc Thesis, 2014, Industrial and Industrial Engineering, Dumlupınar University.

[Behrens 2009] Behrens, S.: Shadow Systems: The Good, The Bad and The Ugly, Communications of the ACM, 2009, 52 (2), 124-129.

[Belletati 2014] Belletati, G.: Building digital workplaces: The BYOD approach, 2014, Università Ca' Foscari Venezia.

[Bengisoy 2017] Bengisoy, A.: Examination of tablet usage by 4 years old pre-school student. World Journal of Environmental Research. 2017, 9 (3), 158-164.

[Bernnat et al. 2010] Bernnat, R., Acker, O., Bieber, N., Johnson, M.: Friendly Takeover, The Consumerization of Corporate IT, 2010, Booz & Company.

[Bock and Ho 2009] Bock, G.W., Ho, S.L.: Non-work related computing (NWRC), Communications of the ACM, 2009, 52(4), 124-128.

[Botha et al. 2009] Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: examining the security experience, Computers & Security, 2009, 28(3), 130–137.

[Burt 2011] Burt, J.: BYOD trend pressures corporate networks, eWeek, 2011, 28 (14), p. 30.

[Büyüköztürk 2009] Büyüköztürk, Ş.: Sosyal bilimler için veri analizi el kitabı istatistik, araştırma deseni - SPSS uygulamaları ve yorum. (10th ed.), 2009, Ankara: Pegem Akademi.

[Carideo et al. 2013] Carideo, J.W., Walker, T.P., Williams, J.C.: A feasibility study of implementing a bring your own computing device policy. PhD Thesis, Naval Postgraduate School, 2013, Monterey, California.

[Chen and Nath 2011] Chen, L., Nath, R.: Impediments to mobile work: an empirical study, International Journal of Mobile Communications, 2011, 9(5), 522–540.

[Child 2006] Child, D.: The essentials of factor analysis. (3rd ed.), 2006, London: Continuum.

[Chou et al. 2008] Chou, C.H., Sinha, A.P., Zhao, H.: A text mining approach to Internet abuse detection, Information Systems and e-Business Management, 2008, 6(4), 419-439.

[Chou et al. 2017] Chou, P.N., Chang, C.C., Lin, C.H.: BYOD or not: A comparison of two assessment strategies for student learning. Computers in Human Behavior, 2017, 74(2017), 63-71.

[Couture 2010] Couture, E.: Mobile security: Current threats and emerging protective measures, 2010, Whitepapers, SANS Institute.

[Çokluk et al. 2010] Çokluk, O., Şekercioğlu, G., Büyüköztürk, S.: Sosyal bilimler için çok değişkenli istatistik: SPSS ve lisrel uygulamaları (1st ed.), 2010, Ankara: Pegem Akademi.

[Emery 2012] Emery, S.: Factors for consideration when developing a bring your own device (BYOD) strategy in higher education, PhD Thesis, 2012, Applied Information Management and the Graduate School of the University of Oregon.

[Fitzgerald, 2009] Fitzgerald, J.: Managing mobile devices. Computer Fraud & Security, 2009, (4), 18–19.

[French et al. 2014] French, A.M., Guo, C., Shim, J.P.: Current Status, Issues, and Future of Bring Your Own Device (BYOD), Communications of the Association for Information Systems, 2014, 35 (10), 191-197.

[Furnell et al. 2006] Furnell, S., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: A survey of end-users, Computers & Security, 2006, 25(1), 27–35.

[Garcia 2013] Garcia, D.A.: Study, analysis and implementation of an enterprise mobility management system, 2013, PhD Thesis, Universitat Politècnica de Catalunya.

[Giddens and Tripp 2014] Giddens, L., Tripp, J.: It's my Tool, I Know How to Use It: A Theory of the Impact of BYOD on Device Competence and Job Satisfaction, 2014, Americas Conference on Information Systems (AMCIS), Savannah, GA, USA.

[Györy et al. 2012] Györy, A., Cleven, A., Uebernickel, F., Brenner, W.: Exploring The Shadows: IT Governance Approaches to User-Driven Innovation, European Conference on Information Systems (ECIS), 2012, Barcelona, Spain.

[Harris et al. 2012] Harris, J., Ives, B., Junglas, I.: IT Consumerization: When Gadgets Turn into Enterprise IT Tools, MIS Quarterly Executive, 2012, 11(3), 99–112.

[Herand and Çalışır 2014] Herand, D., Çalışır T.: The role of software for the improvement of intracompany communication, Kafkas University Journal of Economics and Administrative Sciences Faculty, 2014, 5(8), 67–78.

[Hovav and Putri 2016] Hovav, A., Putri, F.F.: This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. Pervasive and Mobile Computing, 2016, 32, 35-49.

[Hu et al. 2011] Hu, Q., Xu, Z., Dinev, T., Ling, H.: Does deterrence work in reducing information security policy abuse by employees?, Communications of the ACM, 2011, 54(6), 54-60.

[Huang, 2013] Huang, J.Y.: A study on the intention for corporations adapting BYOD policy in Taiwan, MSc Thesis, 2013, Department of Information and Communications, Shih Hsin University.

[Hutcheson and Sofronio 1999] Hutcheson, G.D., Sofronio, N.: Multivariate social scientist: introductory statistics using generalized linear models, 1999, Thousand Oaks, CA: Sage.

[Karasar 2013] Karasar, N.: Bilimsel araştırma yöntemi, 2013, Ankara: Nobel Yayın Evi.

[Kline 1994] Kline, P.: An easy guide to factor analysis, 1994, London: Routledge.

[Kocakoyun and Bicen 2017] Kocakoyun, S., Bicen, H.: Development and Evaluation of Educational Android Application. Cypriot Journal of Educational Science, 2017, 12(2), 58-68.

[Kocamustafaoğulları 2013] Kocamustafaoğulları, M.: A prototype for assessment of information security awareness and implementation level, MSc Thesis, 2013, Graduate School of Natural and Applied Sciences, Çankaya University.

[L.- Vandelannoitte 2015] Leclercq-Vandelannoitte, A.: Managing BYOD: How Do Organizations Incorporate User-Driven IT Innovations?, Information Technology & People, 2015, 28 (1), 2-33.

[Lee and Lee 2002] Lee, J., Lee, Y.: A holistic model of computer abuse within organizations, Information management & computer security, 2002 10(2), 57-63.

[Leech et al 2005] Leech, N.L., Barrett, K.C., Morgan, G.A.: SPSS for intermediate statistics: Use and interpretation (2th ed.), 2005, New Jersey: Lawrence Erlbaum Ass.

[Lüker et al. 2016] Lüker, N., Winkler, T.J., Kude, T.: IT Consumerization and Compliant Use: Do Policies Matter?. PACIS 2016 Proceedings, 2016, Paper 32.

[MacKenzie et al 2011] MacKenzie, S.B., Podsakoff, P. M., Podsakoff, N.P.: Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques, MIS quarterly, 2011, 35(2), 293-334.

[Manz and Stewart 1997] Manz, C.C., Stewart, G.L.: Attaining flexible stability by integrating total quality management and socio–technical systems theory, Organization Science, 1997, 8(1), 59–70.

[Morrow 2012] Morrow, B.: BYOD Security Challenges: Control and Protect Your Most Sensitive Data. Network Security, 2012, 2012 (12), 5-8.

[Moyer 2013] Moyer, J.E.: Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage, Journal of Hospital Librarianship, 2013, 13 (3), 197-208.

[Namlu and Odabasi 2007] Namlu, A.G., Odabasi, F.: Unethical computer using behaviour scale: A study of reliability and validity on Turkish university students, Computers & Education, 2007, 48(2), 205–215.

[Niehaves et al. 2012] Niehaves, B., Köffer, S. Ortbach, K.: IT Consumerization: A Theory and Practice Review, Americas Conference on Information Systems (AMCIS), 2012, Seattle, WA, USA.

[Ortbach et al. 2013] Ortbach, K., Köffer, S., Bode, M., Niehaves, B.: Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior, In: Thirty Fourth International Conference on Information Systems (ICIS), 2013, Milan, ITA.

[Ozdamli and Tavukcu 2016] Ozdamli, F., Tavukcu, T.: Determination of Secondary School Students' Attitudes towards Tablet PC Supported Education. J. UCS, 2016, 22(1), 4-15.

[Phillips 2012] Phillips, J.: Performance testing of mobile applications with multiple technologies, Technical Report, 2012, Florida International University, U.S. Department of Energy.

[Pitichat 2013] Pitichat, T.: Smartphones in the workplace: Changing organizational behavior, transforming the future, LUX: A Journal of Transdisciplinary Writing and Research from Claremont Graduate University, 2013, 3(1), 13.

[Putri and Hovav 2014] Putri, F., Hovav, A.: Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory, European Conference on Information Systems (ECIS), 2014, Tel Aviv, Israel.

[Ruggiero and Foote 2011] Ruggiero, P., Foote, J.: Cyber threats to mobile phones, United States Computer Emergency Readiness Team, 2011, 1–6.

[Ryan et al. 2013] Ryan, H., Ton, M., Keller, E.: Active security, In: Twelfth ACM Workshop on Hot Topics in Networks College Park, 2013, MD, USA.

[Sarıkoz 2015] Sarıkoz, B.G.: An information security framework for web services in enterprise networks. MSc Thesis, 2015, Graduate School of Informatics, Middle East Technical University.

[Sarker et al 2012] Sarker, S., Xiao, X., Sarker, S., Ahuja, M.: Managing Employees' Use of Mobile Technologies to Minimize Work-Life Balance Impacts, MIS Quarterly Executive, 2012, 11(4).

[Schalow et al. 2013] Schalow, P.R., Winkler, T.J., Repschlaeger, J., Zarnekow, R.: The Blurring Boundaries of Work-Related and Personal Media Use: A Grounded Theory Study on the Employee's Perspective, In ECIS, 2013, (paper: 212).

[Şencan 2005] Şencan, H.: Sosyal ve davranışsal ölçümlerde güvenilirlik ve geçerlilik, 2005, Ankara: Seçkin Yayıncılık.

[Shepherd and Klein 2012] Shepherd, M.M., Klein, G.: Using deterrence to mitigate employee Internet abuse, In System Science (HICSS), 2012, 45th Hawaii International Conference on (pp. 5261-5266). IEEE.

[Silic and Back 2014] Silic, M., Back, A.: Shadow IT: A View from Behind the Curtain", Computers & Security, 2014, 45, 274-283.

[Sipahi et al 2013] Sipahi, B., Yurtkoru, E.S., Çinko, M.: Sosyal bilimlerde spss'le veri analizi. (5th ed.), 2013, İstanbul: Beta Yayınları.

[S.- Threlkeld 2011] Steinert-Threlkeld, T.: BYOD: Save money, gain productivity. In Money Management Executive, 2011, 19 (46), 1-10.

[Tavşancıl 2010] Tavşancıl, E.: Tutumların ölçülmesi ve SPSS ile veri analizi, 2010, Ankara: Nobel Yayın Dağıtım.

[Tokuyoshi 2013] Tokuyoshi, B.: The Security Implications of BYOD. Network Security, 2013 (4), 12-13.

[Ugrin and Pearson 2008] Ugrin, J.C., Pearson, J.M.: Exploring Internet abuse in the workplace: how can we maximize deterrence efforts?, Review of Business, 2008, 28(2).

[Uzunboylu and Tugun 2016] Uzunboylu, H., Tugun, V.: Validity and Reliability of Tablet Supported Education Attitude and Usability Scale. J. UCS, 2016, 22(1), 82-93.

[Vogel et al 2010] Vogel, R., Koçoğlu, T., Berger, T.: Consumerization, In Desktopvirtualisierung, 2010, 25-28, Vieweg+ Teubner.

[Walton 1999] Walton, R.E.: From control to commitment in the workplace. Human Resource Management: Critical Perspectives on Business and Management, 1999, 1, 14–29.

[Weiß and Leimeister 2012] Weiß, F., Leimeister, J.M.: Consumerization - IT Innovations from the Consumer Market as a Challenge for Corporate IT, Business & Information Systems Engineering, 2012, 4 (6), 363–366.

[Yılmaz 2014] Yılmaz, V.: Bring your own device "System design based on data security." MSc Thesis, 2014, Graduate School of Natural and Applied Sciences, Beykent University.

[Zhang et al 2006] Zhang, D., Oh, L.B., Teo, H.H.: An experimental study of the factors influencing non-work related use of IT resources at workplace, In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006, IEEE.

Appendix

BYOD Scale to Measure Readiness Level

The personal devices and applications are sufficient for BYOD.
The infrastructure provided for your personal devices is sufficient for high-toned uninterrupted connection and access to data.
BYOD will be the most common implementation in our country in the short term.
The use of personal devices and applications for business purposes will be beneficial to the employees.
The use of personal devices and applications for business purposes will improve the performance of the employees.
The use of personal devices and applications in the workplace will be beneficial to the employers.
BYOD programme will be beneficial to employers and employees.
BYOD and security measuring instruments, it is necessary to make sure that the devices and applications that employees use are up-to-date to protect the corporate networks and data.
BYOD and security measuring instruments, the number of devices on the network should be restricted to protect the corporate networks and data.
BYOD and security measuring instruments, private virtual networks and virtual desktops should be used to protect the corporate networks and data.
In order to protect the BYOD related measuring instruments, corporate networks and the data, location tracking software should be installed to the personal devices.
BYOD and security measuring instruments, employers should be restricted to downloading unsecure applications to protect the corporate networks and data.
Companies BYOD will remain incapable of tracking lost/stolen devices.
Companies BYOD will fall short in terms of management/support.
Companies BYOD will fall behind in terms of the use of personal devices and applications.
Companies BYOD will fall short in terms of cost.
BYOD/A puts more responsibility on employees as a result of the use of personal devices for work.
BYOD makes the character analysis of the employers easier for companies.
BYOD increases the number of smart devices used in business.
BYOD helps employees adapt to workplace environment more easily as they are used to their own devices and applications.