https://doi.org/10.48009/1_iis_2017_11-21

SECURITY POLICIES AND DATA PROTECTION OF MOBILE DEVICES IN THE WORKPLACE

Alex Koohang, Middle Georgia State College, alex.koohang@mga.edu
Maria Teresa Riggio, LUM Jean Monnet University, riggio@lum.it
Joanna Paliszkiewicz, Warsaw University of Life Sciences, joanna_paliszkiewicz@sggw.pl
Jeretta Horn Nord, Oklahoma State University, jeretta.nord@okstate.edu

ABSTRACT

Using mobile devices in and outside the workplace has become the norm, creating a security concern for many companies. It is now commonplace for employees to use multiple mobile devices including smartphones, tablets, and laptops. This study investigated the leading mobile device security issues - according to the literature - regarding security policies and data protection within organizations in the USA and Italy. Results from each country and a comparison between the two were analyzed and are reported in this paper. A discussion of findings, practical implications, recommendations, and limitations complete the paper.

Keywords: Mobile Technology, mobile devices security, security policy, data protection

INTRODUCTION

Mobile technology dominates the way we work, play, and live. The increasing use of mobile devices in the workplace and the mobility, flexibility, and apps that are readily available through mobile devices have allowed companies to remain competitive in a world where employees no longer have to be at their desks to be productive. Using mobile devices in the workplace is not without its' drawbacks. As the use of mobile devices become more and more popular in organizations, their increased vulnerability to security threats and risk becomes a critical issue requiring constant protection and security. The primary goal of this paper is to identify critical security issues regarding policies and data protection of mobile devices within organizations and to find out whether there are significant differences between several selected variables and users' opinions regarding security policies and data protection of mobile device in their organizations. This paper is organized as follows: 1) A review of the literature that identifies eight leading mobile device issues regarding security policies and data protection within organizations; 2) The study's methodology and purpose of the study; and 3) Results, discussion of findings, practical implications, recommendations, and limitations.

ISSUES CONCERNING SECURITY POLICIES AND DATA PROTECTION OF MOBILE DEVICES

For the purpose of this study, eight leading mobile device critical issues regarding security policies and data protection in the workplace were identified. These issues include: 1) policies on "bring your own device" -- BYOD; 2) policies on security of corporate communication; 3) securing mobile apps used; 4) disaster recovery plan for a data breach; 5) deployment of mobile device management - MDM; 6) policies on restrictions of corporate data accessed; 7) enforcing security measures to access sensitive and/or confidential data; and 8) security software that protects data. Following is a brief discussion of each issue based on a review of the literature.

Workplace Policy on BYOD Use Agreement

Today, many employers allow and often encourage employees to use their own devices (such as smartphones, tablets, and laptops) at work, for both personal and professional needs. (Miller et al., 2012; Longo, 2013; Marshall, 2014). There are benefits and risks related to using the BYOD (bring your own device) policy. Often, employees have the flexibility and freedom to choose a mobile device to use at work (either personal or the one provided by their employer). Employers can save money if personal mobile devices are used by the employees to conduct business activities (Ghosh et al., 2013). Another benefit of BYOD is the ability of employees to work from anywhere outside the work environment (Fiorenza, 2013). The BYOD, however, has disadvantages that are related to information security and legal issues (Totten & Hammock, 2014). A lost or stolen device can present a significant risk to the enterprise and customers including data breach, loss of intellectual property, loss of trade secrets, and loss of personal information. Malware is another threat that faces BYOD. Malware is a software that is intended to damage, immobilize, or gain access to a device without the user's knowledge (Totten & Hammock, 2014). To minimize or eliminate the risk from the BYOD strategy, employers must have and abide by a comprehensive policy. According to Totten & Hammock (2014), the policy must define the scope of covered devices, appropriate use, cost, and support issues. In addition, the policy must include implementation of security protocols; outline the consequences for violations; contain a mechanism for monitoring employee access and appropriate use; and require training for all employees.

Workplace Policy on Security of Corporate Communication

According to Goodman (2004), corporate communication is the term used to describe a variety of strategic management functions. The corporate communication within an organization includes "... public relations; crisis and emergency communication; corporate citizenship; reputation management; community relations; media relations; investor relations; employee relations; government relations; marketing communication; management communication; corporate branding and image building; and advertising" (Goodman, 2006, p. 197). Mobile devices use various apps for corporate communication. Unfortunately, some of these apps may not be designed with security and privacy in mind, and they pose a variety of security risks to mobile users and their enterprises (Ajami et al., 2011; He, 2012). Therefore, organizations must have a sound policy for corporate communication via mobile devices.

Securing Mobile Apps used in the Workplace

Researchers have confirmed that enterprise data are increasingly distributed across mobile devices and the IT departments within organizations are struggling to secure private corporate data (e.g., He, 2012; Wu, 2013). IT departments often have little control over employees' mobile devices especially when they are using their own devices to conduct business activities. The installed apps on personal mobile devices pose tremendous security threats, i.e., viruses, worms, or Trojan horses. Security risks and threats caused by these apps are serious challenges facing enterprises. Often, some enterprises do not have sufficient mechanisms to secure mobile apps on personal mobile devices in the workplace (Huang et al., 2007).

Workplace Disaster Recovery Plan for Data Breach

The most obvious risk related to using mobile devices is the loss or theft of data. A lost or stolen device, especially without security settings like passwords, can result in a data breach that may carry significant legal and reputational costs (Totten & Hammock 2014). It is important that organizations establish a disaster recovery plan for a data breach. According to Choo (2011), a good disaster recovery plan should clearly specify required steps to reporting and managing incidents such as loss of mobile devices, possible compromise of passwords, information leak, data breaches, and viruses/malware attacks. The plan should also include how to mitigate the risks.

Workplace Deployment of Mobile Device Management (MDM)

According to Harris and Patten (2014), a mobile device management (MDM) is a type of security software that monitors, manages and secures mobile devices within the workplace. It can be deployed to secure multiple mobile platforms across multiple mobile operating systems. The vital functions of an MDM include software deployment, i.e., patch deployment, configuration management, etc. Additionally, an MDM can locate, troubleshoot backup, lock and wipe clean a mobile device remotely (Wu, 2013). Miller et al. (2012) asserted that if employees use their own devices for organizational purposes it means that enterprises do not always own or control the software to be installed on the employees' mobile devices and it is much harder to enforce security policies on such devices. According to Wu (2013), enterprises will need to strengthen user education to support their MDM solutions.

Workplace Policy on Restrictions of Corporate Data Accessed

Mobile devices allow employees to conduct business from anywhere. This allows for flexibility, efficiently, and rapid response to corporate issues requiring immediate attention (Markelj & Bernik, 2014). Various networks such as Wi-Fi, UMTS, and LTE enable users to access information from anywhere whether stored in a central information system or in a cloud (Markelj & Bernik 2014). As mobile devices and mobile networks continue to evolve and improve, it is important for organizations to create workplace policy on restrictions of corporate data accessed, which should clarify acceptable use of mobile devices. This should be paired with employee education aimed at promoting risk awareness. Risky behavior includes downloading apps from online stores that may not be trusted, turning off security settings, not reporting lost devices that may contain confidential and sensitive information (Ponemon Institute, 2012; Bankosz & Kerins, 2014)

Enforcing Security Measures for Accessing Sensitive and/or Confidential Data

NIST (2013) supports three security measures for mobile devices. They are confidentiality, integrity, and availability. These security measures may be taken to secure mobile devices against threats. Enforcing security measures for accessing sensitive and confidential data within organizations requires a set of clear guidelines within organizations. NIST (2013) recommended six guidelines to secure mobile devices within organizations. These guidelines are:

1. "Organizations should have a mobile device security policy.
2. Organizations should develop system threat models for mobile devices and the resources that are accessed through the mobile devices.
3. Organizations deploying mobile devices should consider the merits of each provided security service, determine which services are needed for their environment, and then design and acquire one or more solutions that collectively provide the necessary services.
4. Organizations should implement and test a pilot of their mobile device solution before putting the solution into production.
5. Organizations should fully secure each organization-issued mobile device before allowing a user to access it.
6. Organizations should regularly maintain mobile device security." (NIST, 2013, pp.1-23)

Security Software that Protects Data

The security software controls and alerts unauthorized access to the wireless information transmission channels, obtaining privileges, copying applications or stealing intellectual property, prevents individuals from downloading malicious content and protects user's data from being sent to the third parties and its improper use (Main, 2004). According to Martin & Rice (2011), a key mechanism for dealing with the online threats was the installation and regular update of security software. Unfortunately, many people do not protect their mobile devices and do not install the security software such as antivirus and firewall software. Barrera & Van Oorschot, (2011) underline that IT staff in enterprises should support employees with security software installation and update. Organizations can use secure gateway technologies to analyze web traffic to detect malware and reduce the risk of malware infection and data loss (Wu, 2013).

PURPOSE OF THE STUDY

As revealed and discussed in the review of the literature, eight leading issues were identified for this study regarding security policies and data protection of mobile devices within organizations.

The eight security policies and data protection of mobile devices within organizations were placed into one group and treated as the dependent variable (DV = Security policies and data protection of mobile devices). Next, seven independent variables of interest were identified, namely, IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement, IV_3 = Mobile device used in the workplace, IV_4 = Likelihood of using mobile devices, IV_5 = Time spent using mobile devices, IV_6 = Age, and IV_7 = Gender. As a result, we aimed to answer the following research question (RQ):

RQ: Are there significant mean differences between the independent variables (IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement, IV_3 = Mobile device used in the workplace, IV_4 = Likelihood of using mobile devices, IV_5 = Time spent using mobile devices, IV_6 = Age, and IV_7 = Gender) and the dependent variable (DV = Security policies and data protection of mobile devices)?

METHODOLOGY

Instrument

The instrument used for this study consisted of two parts. Part one included the demographic questions. Part two was comprised of eight Likert-type statements about mobile devices security policies and data protection within organizations. These items were deemed important by a panel of experts that included four university professors as well as a review of recent literature on security policy and data protection on mobile devices issues. The items of the instrument were as follows:

1. My company has a clear policy on the security of BYOD (Bring Your Own device) in the workplace.
2. My company has a clear policy on the security of corporate communication conducted on mobile devices.
3. My company has implemented steps to secure the vulnerability of mobile apps I use in the workplace.
4. My company has a disaster recovery plan in case I experience a data breach.
5. I am aware of my company's deployed Mobile Device Management (MDM) that secures, monitors, manages, and supports my activities on mobile devices.
6. My company places restrictions on corporate data that may be accessed by employees using personal and/or corporate mobile devices.
7. My company has a good handle on enforcing security measures to access sensitive and/or confidential data via mobile devices.
8. Security software that protects data on my mobile device is constantly updated.

The instrument used the following measuring scale: 7 = Completely Agree, 6 = Mostly Agree, 5 = Somewhat Agree, 4 = Neither Agree nor Disagree, 3 = Somewhat Disagree, 2 = Mostly Disagree, and 1 = Completely Disagree.

Subjects and Procedure

The sample population for this study was chosen from two different countries: The USA (N = 128, 49% female and 51% male) and Italy (N = 118, 54% female and 46% male). The age categories of subjects from the USA were 21 - 29, 18.0%, 30 - 39, 21.9%, and 40 or older, 60.2%. The age categories of the subjects from Italy were 21 - 29, 19.5%, 30 - 39, 26.3%, and 40 or older, 54.2%. Additional demographics data are shown in Table 1.

The samples from these two countries were not chosen for any specific reason. They were chosen because of the convenience and availability of the subjects. Garson (2013) stated that convenience sampling, a type of non-probability sampling technique, is a standard process of collecting data. The author asserted that a convenience sample 1) is easy to access, 2) reduces cost, 3) reduces collection time, 4) reduces rules on how to collect data, and 5) gathers useful data that may not be achievable using probability sampling techniques. The instrument was administered online to the subjects from the USA and Italy. Subjects from both countries were assured anonymity and confidentiality.

Table 1. Demographics -- USA & Italy

Number of employees				
	USA		Italy	
	Freq.	%	*Freq.*	%
0-250	61	47.7	71	60.2
251-500	10	7.8	6	5.1
501-750	10	7.8	7	5.9
751-1000	47	36.7	3	2.5
1000 +	0	0	31	26.3
Type of organizations				
	USA		Italy	
	Freq.	%	*Freq.*	%
Private	80	62.5	116	98.3
Public	48	37.5	2	1.7
Mobile device operating systems used				
	USA		Italy	
	Freq.	%	*Freq.*	%
Apple iOS	52	40.6	16	13.6
Android	23	18.0	19	16.1
Windows	20	15.6	32	27.1
Combination	33	25.8	51	43.2
Mobile device used to conduct company business				
	USA		Italy	
	Freq.	%	*Freq.*	%
Smartphone	46	35.9	23	19.5
Tablet	7	5.5	4	3.4
Laptop	42	32.8	52	44.1
Combination	33	25.8	39	33.1
Company BYOD Policy				
	USA		Italy	
	Freq.	%	*Freq.*	%
Company Only	40	31.3	36	30.5
Employee Only	49	38.3	24	20.3
Company & Employee	39	30.5	58	49.2
Likely use a mobile devices in the Workplace				
	USA		Italy	
	Freq.	%	*Freq.*	%
Extremely likely	71	55.5	76	64.4
Very likely	18	14.1	24	20.3
Moderately likely	11	8.6	12	10.2
Slightly likely	15	11.7	6	5.1
Not at all likely	13	10.2	0	0
Time spent using a mobile devices for business activities				
	USA		Italy	
	Freq.	%	*Freq.*	%
1 - 2 Hours	57	44.5	41	34.7
3 - 4 Hours	25	19.5	22	18.6
5 - 6 Hours	19	14.8	19	16.1
Over 6 hours	27	21.1	36	30.5

Data Analysis

Univariate Analysis of Variances was used to answer the research question. This procedure is used where there are multiple independent variables with one dependent variable. The independent variables were as follows: IV_1 = types of operating system used, IV_2 = types of mobile devices used, IV_3 = BYOD policy, IV_4 = age, and IV_5 = gender. The dependent variable was DV = mobile devices security. The analysis assumes that 1) the dependent variable is continuous and each independent variable is comprised of two or more levels; 2) there will be no relationship between the observations in each group or between the groups; and 3) outliers should be eliminated from the data (Mertler & Vannatta, 2010). After these assumptions are fulfilled, data are tested for homogeneity of variances using Levene's test. Levene's test determines equality of variances of the data. A non-significant value from the Levene's test indicates homogeneity of variance. The F value calculated (from the univariate analysis of variance) for each independent variable determines the significance of the groups on the dependent variable. Post hoc analysis is conducted for groups with more than two levels if found significant. Descriptive analyses are performed to show the means and standard deviation of the dependent variable with each independent variable.

RESULTS

The following assumptions were fulfilled prior to conducting the actual data analysis: the dependent variable was continuous, each independent variable consisted of two or more levels, and there was no relationship between the observations in each group or between the groups. Additionally, outlier analyses on data for both the USA and Italy were conducted to eliminate (if any) unusual or extreme values at one or both ends of the data distribution. Three cases from the original data from the USA (N = 131) and two cases from the original data from Italy (N = 120) were found to have unusual or extreme multivariate outlier. They were then eliminated, yielding a final sample of N = 128 for the USA and a final sample N = 118 for Italy.

Descriptive analysis

Figure 1 depicts the descriptive analysis comparing the means of each item of the dependent variable (Security policies and data protection of mobile devices). The results revealed higher mean scores for all eight items reported by the subjects from Italy.

Univariate ANOVA - USA

Levene's test for the set of data for the USA showed a non-significant value ($p = .467$) indicating homogeneity of variance. The results of the univariate ANOVA for the USA are shown in Table 2.

Non-significant variables: There were no significant mean differences reported between the independent variables of IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement, IV_3 = Mobile device used in the workplace, IV_4 = Likelihood of using mobile devices, IV_6 = Age, IV_7 = Gender and the dependent variable of DV = Security policies and data protection of mobile devices.

Significant variable: There were significant mean differences reported between the independent variables of IV_5 = Time spent using mobile devices and the dependent variable of DV = Security policies and data protection of mobile devices.

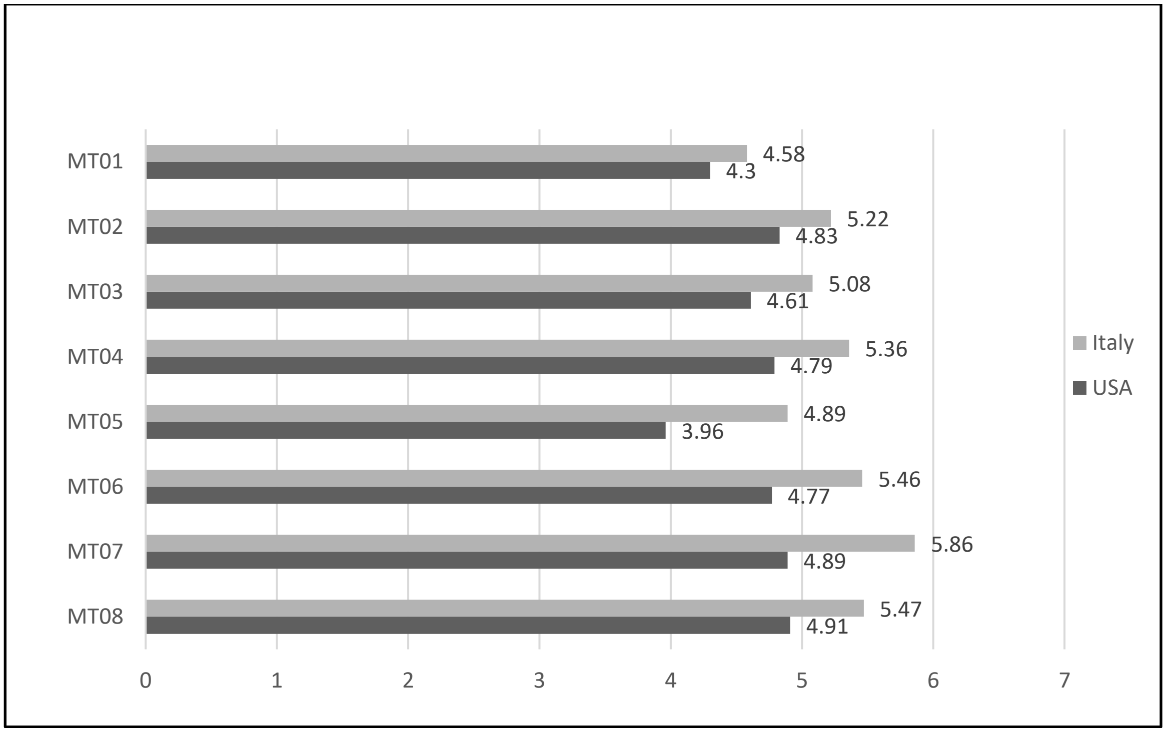

Figure 1. Descriptive analysis - Italy and the USA

MT01 = Workplace policy on BYOD use, MT02 = Workplace policy on security of corporate communication, MT03 = Securing mobile apps used in the workplace, MT04 = Workplace disaster recovery plan for data breach, MT05 = Workplace deployment of Mobile Device Management (MDM), MT06 = Workplace policy on restrictions on corporate data accessed, MT07 = Enforcing security measures to access sensitive and/or confidential data in the workplace, and MT08 = Security software that protects data

Table 2. Univariate ANOVA - USA

	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	67.936[a]	18	3.774	1.414	.139
Intercept	780.565	1	780.565	292.414	.000
IV_1 *Mobile device operating systems*	5.764	3	1.921	.720	.542
IV_2 *BYOD use agreement*	.679	2	.339	.127	.881
IV_3 *Mobile device used in workplace*	1.302	3	.434	.163	.921
IV_4 *Likelihood of using mobile devices*	12.551	4	3.138	1.175	.326
IV_5 *Time spent using mobile devices*	22.181	3	7.394	2.770	**.045**
IV_6 *Age*	.184	2	.092	.034	.966
IV_7 *Gender*	7.538	1	7.538	2.824	.096
Error	290.963	109	2.669		
Total	3106.156	128			
Corrected Total	358.898	127			

a. R Squared = .189

The means for IV_5 = Time spent using mobile devices and the dependent variable of DV = Security policies and data protection of mobile devices were 1 - 2 Hours, N = 57, 4.109; 3 - 4 Hours, N = 25, 4.541; 5 - 6 Hours, N= 19, 5.289; and Over 6 hours, N= 27, 5.115. The post hoc comparisons results for the IV_5 = Time spent using mobile devices

Volume 18, Issue 1, pp. 11-21, 2017

and the dependent variable of DV = Security policies and data protection of mobile devices were as follows: (1 - 3 & 3 - 1 = -1.179) (1 - 4 & 4 - 1 = -1.006).

Univariate ANOVA - Italy

Levene's test for the set of data for Italy showed a non-significant value (p = .207) indicating homogeneity of variance. The results of univariate ANOVA for Italy are shown in Table 3.

Non-significant variables: There were no significant mean differences reported between the independent variables of, IV_3 = Mobile device used in the workplace, IV_4 = Likelihood of using mobile devices, IV_5 = Time spent using mobile devices, IV_6 = Age, IV_7 = Gender and the dependent variable of DV = Security policies and data protection of mobile devices.

Significant variable: There were significant mean differences reported between the independent variables of IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement and the dependent variable of DV = Security policies and data protection of mobile devices.

Table 3. Univariate ANOVA – Italy

	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	45.738[a]	17	2.690	2.346	.005
Intercept	580.388	1	580.388	505.987	.000
IV_1 *Mobile device operating systems*	9.816	3	3.272	2.853	**.041**
IV_2 *BYOD use agreement*	8.237	2	4.118	3.590	**.031**
IV_3 *Mobile device used in workplace*	2.235	3	.745	.649	.585
IV_4 *Likelihood of using mobile devices*	7.543	3	2.514	2.192	.094
IV_5 *Time spent using mobile devices*	2.372	3	.791	.689	.561
IV_6 *Age*	6.629	2	3.315	2.890	.060
IV_7 *Gender*	.026	1	.026	.023	.880
Error	114.704	100	1.147		
Total	3401.016	118			
Corrected Total	160.442	117			

a. R Squared = .285

The means for IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement and the dependent variable of DV = Security policies and data protection of mobile devices are as follows:

- IV_1 -- Apple iOS, N = 16, 5.565; Android, N = 19, 4.532; Windows, N = N = 32, 5.185; and Combination, N = 51, 5.247.
- IV_2 -- Company Only, N = 36, 5.521; Employee Only, N = 24, 4.715; and Company & Employee, N = 58, 5.160.

The post hoc comparisons results for IV_1 = Mobile device operating systems and the dependent variable of DV = Security policies and data protection of mobile devices were as follows: (1 - 2 & 2 - 1 = 1.033) (2 - 3 & 3 - 2 = -.653) (2 - 4 = -.715) (4 - 2 = .715). The post hoc comparisons results for IV_2 = BYOD use agreement and the dependent variable of DV = Security policies and data protection of mobile devices were as follows: (1 - 2 & 2 - 1 = .806).

DISCUSSION

Demographics

Subjects from both the USA and Italy were surveyed regarding security policies and data protection of mobile devices used in the workplace. Results are representative of both small and large companies with 47.7 percent of the respondents from the USA and over 60 percent of the respondents from Italy working in companies with less than 250 employees. Results further revealed that one-third of the respondents from the USA work in companies ranging from 751-1000 employees and over one-fourth of the respondents from Italy work in companies with 1000 or more employees. The majority of respondents work in private companies with the gender division of the respondents fairly equal in both the USA and Italy. Over 50 percent of respondents from both countries were 40 years of age and older. The next largest age group of respondents was 30-39 years.

The Apple iOS was ranked highest among the mobile device operating systems listed by respondents in the USA while Windows was ranked highest by respondents in Italy. This is not a surprise considering that the smartphone was indicated as the most used mobile device in the USA and the laptop was indicated as the top mobile device used by those in Italy. *Employee only* was the preferred method for ownership of mobile devices in the workplace by those in the USA while a combination of *employee and company mobile phones* was the method ranked highest by the respondents from Italy.

A large percentage (55.5 percent in the USA) and (66.4 percent in Italy) indicated that they were extremely likely to use mobile devices in the workplace. More than 40 percent of the USA respondents and over 30 percent of the respondents from Italy use a mobile device for business activities for 1-2 hours per day, while over 20 percent (USA) and more than 30 percent (Italy) spend six or more hours a day on a mobile device for business purposes.

Descriptive Analysis - Items of the Dependent Variable

When comparing the mean values of the items of the dependent variable, results revealed that in general subjects from both the USA and Italy did not express a high viewpoint about security policies and data protection of mobile devices in the workplace. As depicted in Figure 1, the mean scores for all items were above average or slightly above average. A conclusion that may be drawn from this result is that the security policies and data protection of mobile devices in the workplace are not perceived as the highest organizational priorities. Interestingly, slightly higher mean scores were reported by the subjects from Italy for all eight items regarding security policies and data protection of mobile devices/technology. The highest percentage reported by subjects from Italy was on MT07-- Enforcing security measures to access sensitive and/or confidential data in the workplace and the second highest results by Italy were on MT08 -- Security software that protects data. Ironically, similar results were revealed by the USA with MT08 -- Security software that protects data slightly ahead of MT07 -- Enforcing security measures to access sensitive and/or confidential data in the workplace. Future studies should consider further examining these items.

Significant Group Differences

The research question that stated whether significant mean differences between the independent variables (IV_1 = Mobile device operating systems, IV_2 = BYOD use agreement, IV_3 = Mobile device used in the workplace, IV_4 = Likelihood of using mobile devices, IV_5 = Time spent using mobile devices, IV_6 = Age, and IV_7 = Gender) and the dependent variable (DV = Security policies and data protection of mobile devices) for subjects from the USA and Italy were answered through conducting two separate univariate analysis of variance. For subjects from the USA, the amount of *time spent using mobile devices* appeared to be a significant variable in relation to their view of security policies and data protection of mobile devices in the workplace. Subjects who spent more time using mobile devices to conduct business activities had significantly higher mean scores. Therefore, the following question merits further research -- Is it possible that subjects from the USA who spend more time using mobile devices to conduct business activities have a higher awareness of security policies and data protection of mobile devices in the workplace?

For subjects from Italy, the type of *mobile device operating system* and the *BYOD use policy/agreement* were significant variables in relation to their view of security policies and data protection of mobile devices in the workplace. Subjects using mobile devices with Apple iOS had significantly higher mean scores. This result is notable because the use of Windows OS as shown in Table 1 was ranked highest by respondents in Italy. Therefore, the following question merits further research -- Is it possible that subjects using mobile devices with Apple iOS have a higher perception of awareness of security policies and data protection of mobile devices in the workplace? Subjects who used the company's mobile device to conduct business activities had significant mean scores. This result is also notable because approximately 30% of the subjects as shown in Table 1 were using mobile devices provided by the company to conduct business activities. Therefore, the following question merits further research -- Is it possible that subjects may prefer using company-provided mobile devices to conduct business activities in the workplace?

Practical Implication of the Results

This study, in general, revealed that subjects from both the USA and Italy did not have high mean scores on any of the eight items regarding security policies and data protection of mobile devices. In other words, the mean scores for all eight items were reported as average or slightly above average for both countries. A critical question should be asked: What measures do organizations take to enforce security policies and data protection of mobile devices? Straub & Welke (1998) asserted that security education training and awareness (SETA) programs are essential for employees to learn and offset threats against security and data breaches. These programs are normally conducted through seminars and workshops to increase employee awareness about security policies and data protection of mobile devices (Straub & Welke, 1998; D'Arcy et al., 2009).

The SETA for mobile devices should be a top strategic priority within organizations. The SETA should be a routine and regular undertaking by organizations that includes a discussion and review of a list of mobile devices security risks and threats to employees and the organization; a review and discussion of mobile device security protocols; the employee commitment and fulfillment of security compliances; sanctions for failing to fully comply with security policies; data protection of mobile devices; and reward for mobile security and data protection compliance.

In addition, a sound SETA for mobile devices should require all employees to participate in training. All materials, whether developed by the organization or purchased from outside sources (online training, webinars, seminars, workshops, etc.) for mobile devices security training and awareness must be relevant and up-to-date. Organizations must regularly and routinely review and assess their security policies and data protection for mobile devices.

REFERENCES

Ajami, R., Ramadan, N., Mohamed, N. & Al-Jaroodi, J. (2011). Security challenges and approaches in online social networks: a survey. *International Journal of Computer Science and Network Security, 11*(8), 1-12.

Bankosz, G. S., & Kerins, J. (2014). Mobile technology-enhanced asset maintenance in an SME. *Journal of Quality in Maintenance Engineering, 20*(2), 163-181.

Barrera, D. & Van Oorschot, P. (2011). Secure software installation on smartphones. *IEEE Security & Privacy, 9*(3), 42-48.

Choo, K. R. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security, 30*(8), 719-731.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79–98.

Fiorenza, P. (2013). Mobile technology forces study of bring your own device. *Public Manager, 42*(1), 12-14.

Garson, D. (2013). *Survey Research & Sampling* (Statistical Associates "blue book" series book 7). Asheboro, NC: Statistical Associate Publishing.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62–70.

Goodman, M. B. (2004). Today's corporate communication function", in Oliver, S.M. (Ed.), *Handbook of Corporate Communication and Public Relations: Pure and Applied,* (pp. 200-227). Routledge, London.

Goodman, M. B. (2006). Corporate communication practice and pedagogy at the dawn of the new millennium. *Corporate Communications, 11*(3), 196-213.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114.

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology, 14*(2), 171-180.

Huang, D.L., Rau, P.L., Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In: *Human–computer interaction: applications and services*, LNCS. Springer, 906–915.

Longo, B. (2013). Learning on the wires: BYOD, embedded systems, wireless technologies and cybercrime. *Legal Information Management, 13*(2), 119-123.

Main, A. (2004). Application security: Building in security during the development stage. *Information Systems Security, 13*(2), 31-37.

Markelj, B., & Bernik, I. (2014). Information security related to the use of mobile devices in slovene enterprises. *Varstvoslovje, 16*(2), 117-127.

Marshall, S. (2014). IT consumerization: A case study of BYOD in a healthcare setting. *Technology Innovation Management Review, 4*(3), 14-18.

Martin, N. and Rice, J. (2011). Cybercrime: understanding and addressing the concerns of stakeholders. *Computers & Security, 30*(8), 803-814.

Mertler, C.A., & Vannatta, R.A. (2010). *Advanced and multivariate statistical methods*. *Los Angeles, CA: Pyrczak*.

Miller, K.W., Voas, J. & Hurlburt, G. F. (2012). BYOD: security and privacy considerations. *IT Professional, 14*(5), 53-55.

NIST (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf Accessed 8 February 2017

Ponemon Institute (2012). Global study on mobility risks: United States, available at: www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf Accessed 8 February 2017.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469.

Totten, J. A., & Hammock, M. C. (2014). Personal electronic devices in the workplace: Balancing interests in a BYOD world. ABA *Journal of Labor & Employment Law, 30*(1), 27-45.

Wu, H. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security, 21*(5), 381-400.