https://doi.org/10.48009/1_iis_2019_1-11

Issues in Information Systems
Volume 20, Issue 1, pp. 1-11, 2019

PREDICTORS OF SUCCESS IN SECURITY AND DATA PROTECTION AWARENESS OF MOBILE DEVICES: TRUST AND PRIVACY

Alex Koohang, Middle Georgia State University, alex.koohang@mga.edu
Joanna Paliszkiewicz, Warsaw University of Life Sciences, joanna_paliszkiewicz@sggw.pl
Jeretta Horn Nord, Oklahoma State University, jeretta.nord@okstate.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu
Tara Underwood, Middle Georgia State University, tara.underwood@mga.edu

ABSTRACT

This study investigates the influence of two predictor variables, i.e., trusting beliefs and privacy concerns in predicting users' security and data protection awareness of mobile devices. A Likert-type instrument with three constructs was administered to the subjects from various organizations in the USA (N = 184). Collected data were analyzed using multiple regression analysis. Results showed that both users' privacy concerns and trusting beliefs were variables of success in predicting the users' security and data protection awareness of mobile devices. Several implications for practice are made. Recommendations for future research are provided.

Keywords: Mobile devices, security, data protection, awareness, trusting belief, privacy concerns

INTRODUCTION

The use of mobile devices in organizations have presented great promise for improved communication and increase efficiency for collaboration and innovative ways for performing day-to-day business activities (Ko & Jeng, 2015). Mobile apps provide great mobility, flexibility, and information dissemination (Nah *et al*., 2005) and they possess vast functionality, good user interface design, as well as adaptability (Lee & Benbasat, 2004, Lee & Shim, 2006). La Polla *et al*. (2013) reported that the mobility and increasing capabilities of mobile devices have significantly contributed to their increased use. Moreover, the mobile devices are beginning to replace personal computers as they can hold and process large volumes of sensitive data which makes them an attractive target for hackers (Leavitt, 2011). The rapid and ubiquitous use of mobile devices has its drawbacks.

Security threats to mobile devices are increasing in frequency (Felt *et al*., 2011; Wu, 2013). These security threats have caused a variety of damages such as information theft, leaking of user privacy as well as personal, financial, and professional losses (Dai *et al*., 2010; Chiang & Tsaur, 2011; Arthur & Boggan, 2011) that present a tremendous concern for organizations (Liang & Xue, 2009). Scholars have confirmed that users tend to ignore security and privacy policies and requirements which increases threats to the organizations' assets (e.g., Mylonas 2013a; Gkioulos, *et al*. 2017; Paullet & Pinchot, 2014). This may be as a result of users not being aware of critical issues related to mobile devices (Koohang *et al*., 2018a). Therefore, awareness of the security issues regarding mobile devices and the variables that may be influential in contributing to employees' following the privacy policies and requirements merit attention.

This paper seeks to determine the variables of success (i.e., trusting beliefs, and privacy concerns) that influence users' security and data protection awareness of mobile devices. We define "security and data protection awareness of mobile devices" as employees' knowledge of critical issues facing security and data protection of mobile devices. "Trusting beliefs" is defined as employees' sense of trust that organization will be trustworthy, thoughtful, keeping promises, and acting consistently in all aspects of security and data protection of mobile devices. "Privacy concerns" is defined as employees' concern about control, access, collection, use, share of their personal information while using mobile devices to perform business activities.

The rest of this paper is structured as follows. First, a review of the literature delineates security and data protection awareness of mobile devices, trusting beliefs, and privacy concerns. Second, the purpose of the study follows the problem statement. Third, the study's methodology is described. This part includes the description of the instrument, sample, procedure, and data analysis. Fourth, results are presented following the discussion of findings, implications, and conclusion.

SECURITY AND DATA PROTECTION AWARENESS OF MOBILE DEVICES

The threats to mobile devices' security and privacy are real and stem from a lost or stolen device (Totten & Hammock, 2014), poorly designed apps (He, 2012), apps on personal mobile devices used as BYOD (Huang *et al*., 2007), not reporting security or data breach incidents (Choo, 2011), lack of MDM (Miller *et al*., 2012) downloading apps, turning off security settings (Bankosz & Kerins, 2014), not regularly updating software and lack of antivirus (Martin & Rice, 2011).

Organizations implement security policies as guidelines and requirement to improve information security and privacy (Ifinedo, 2014). NIST (2017) defined information security policy as the "… aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information." To protect organizations' assets, employees' compliance with security policies and procedures is a necessity (NIST 2017). Therefore, user awareness of security policies becomes essential in safeguarding mobile devices that are being used within organizations for day-to-day business activities because it plays a critical role in promoting security policy and data protection of mobile devices and minimize the threats (Koohang *et al*., 2018a).

Information security awareness is defined as a "state where users in an organization are aware of - ideally committed to - their security mission (often expressed as in end-user security guidelines)" (Siponen, 2000, p. 31). Shaw *et al*. (2009) described information security awareness as "… the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control" (p. 92).

Koohang *et al*. (2017) identified eight critical issues regarding security policies and data protection of mobile devices in organizations. These issues are 1) bring your own device (BYOD) use agreement, 2) security of corporate communication, 3) mobile apps used in the workplace, 4) disaster recovery plan for data breach, 5) use of mobile device management (MDM), 6) restrictions for accessing corporate data, 7) enforcement of security measures for accessing sensitive/confidential data, and 8) security software that protects data. Understanding these critical issues becomes significant in protecting organizations' assets.

PRIVACY CONCERNS

Safeguarding users' privacy is a major challenge in using mobile devices in organizations (Kuo *et al*., 2015). Smith *et al*. (2011) describe privacy as the ability of an individual to control his or her personal information. Malhotra *et al*. (2004) and Smith *et al*. (1996) described privacy concerns as general concerns that reflect individuals' inherent worries about the possible loss of information privacy.

Privacy concerns have been studied when it comes to the benefits or detriments of mobile technology. For example, Shin (2012), revealed issues that pertained to the accuracy of health information being exchanged across wireless connectivity. These were difficulties with inaccurate data, delay of information, the potential for information being received by the wrong patient, limited security features, and vulnerability to unauthorized access were all addressed (Shin, 2012). ITIC (2018) advanced a framework for privacy that state

> "Individuals should have the right to exercise control over the use of their personal data where reasonable to the context surrounding the use of personal data. These individual control rights, consistent with the rights and legal obligations of other stakeholders, include the right to access, correct, port, delete, consent, and object to the use of personal data about themselves." (ITIC, 2018, p. 2)

Concerns about privacy generally lead individuals to be more careful about managing and controlling their personal information (Anderson & Agarwal 2011, Malhotra *et al*. 2004). Companies advertising on mobile applications have access to a large volume of users' personal and private information. They are able to know users' gender, age, home address as well as users' preferences in various matters (Demetriou *et al*. 2016). Xu *et al*. (2009) found that privacy concerns discouraged individuals from disclosing their physical location to the service provider when using mobile devices.

Toch (2014) asserted that users' personal information should be collected and used in a way that is consistent with their expectations. According to Palen and Dourish (2003) users' sense of privacy is correlated with the control they have over their information. In the context of using mobile devices in the workplace, we define privacy concerns 1) personal information and data that are not protected from unauthorized, 2) unauthorized people getting access to personal information and data, 3) not having control over personal information and data when performing business activities, and 4) how personal information is collected, processed, and used while performing business activities.

TRUSTING BELIEFS

Trust plays an important role in facilitating online social and economic exchange (Zhou, 2015; Bapna *et al*., 2017). Corritore *et al*. (2003) defined trust in an online environment as an expectation that a user's vulnerabilities will not be misused and manipulated. Mallat (2007) conducted a qualitative study and confirmed that trust significantly affects the consumer adoption of mobile payment. Vance *et al*. (2008) noted that system quality including navigation structure and visual appeal affects user trust in mobile technologies.

Li and Yeh (2010) found that design aesthetics affect user trust in mobile websites. Apart from this, experience in technology usage, propensity to trust, perceived ease of use, information quality, customization and personalization, good use of visual design elements, privacy and security, third-party guarantees, the presence or absence of visual anchors, interpersonal cues or prominent features, such as a photograph, video/audio, avatar, or trust seal, reputation and offline presence are all relevant determinants for trust (Riegelsberger *et al*., 2005; Sillence *et al*., 2006; Kim, Ferrin & Rao, 2008; Beldad *et al*., 2010; Lin, Lu, Wang & Wei, 2011; Chan, 2012).

In the study conducted by Serrano (2016), professional trust was assessed based upon the patient's perception of the health information that was shared and their reliability on the health care provider's services in meeting their individual medical needs. Mylonas *et al*. (2013b) explore the security awareness of smartphone users and show that users display high levels of trust towards smartphone application repositories, and they rarely consider privacy and security when installing a new application. Koohang *et al*. (2018a) defined trusting beliefs in the context of mobile devices as the organization

> "1) is trustworthy in implementing and executing the security and data protection of mobile devices; 2) keeps employees' best interests in mind when dealing with the security and data protection of mobile devices; 3) fulfills promises related to all aspects of security and data protection of mobile devices; and 4) is predictable and consistent regarding the security and data protection for mobile devices used in the workplace." (p. 7-8)

In general, awareness promotes and encourages openness and communication among employees. Awareness improved openness. It builds an increased trusting environment (Golembiewski & McConkie, 1975). McKnight & Webster (2001) asserted awareness strengthens, shapes, and augments trust among individuals and teams resulting in a feeling of satisfaction.

PURPOSE OF THE STUDY

The purpose of this study is to determine the variables of success (i.e., privacy concerns, and trusting beliefs) in predicting users' security and data protection awareness of mobile devices. Consistent with its purpose, the following research question is asked. *Which of the two predictor variables (trusting beliefs and privacy concerns) are most influential in predicting users' security and data protection awareness of mobile devices?*

METHODOLOGY

Instrument

The Likert-type instrument is comprised of three parts with sixteen items to describe 1) individuals' security policy and data protection awareness of mobile devices, 2) individuals' privacy concerns of mobile devices, and 3) individuals' trusting beliefs about security and data protection of mobile devices.

The first part of the instrument includes eight items that describe the security policy and data protection awareness. They are based on an instrument developed by Koohang *et al*. (2017) that identified the leading issues regarding security policy and data protection of mobile devices in organizations. These issues were BYOD – bring your own device, the security of corporate communication, securing mobile apps used in the workplace, a disaster recovery plan for a data breach. deployment of mobile device management (MDM), restrictions of corporate data accessed, implementing security measures for accessing corporate data, and updating security software to protect data (Koohang *et al*., 2017). Koohang *et al*. (2018a) adapted these eight leading issues in their three-dimension-construct model to reflect on employees' security and data protection awareness of mobile devices. The items are as follows:

1. "I am aware that my company has a clear security policy on "bring your own device" (BYOD) in the workplace.
2. I have sufficient knowledge about my company's security policy regarding corporate communication conducted on mobile devices.
3. I know that my company has implemented appropriate steps to secure mobile apps I use in the workplace.
4. I am aware that my company has a clear policy regarding disaster recovery plan in case I experience [a] security breach on mobile devices I use in the workplace.
5. I am aware of my company's deployed Mobile Device Management (MDM) that secures, monitors, manages, and supports [the] protection of data on mobile devices.
6. I know that my company places restrictions on corporate data that may be accessed by employees using their personal mobile devices.
7. I am aware that my company has a good handle on enforcing security measures to access sensitive and/or confidential data.
8. I have knowledge about frequent updates of security software on all mobile devices used in the workplace to protect data." (Koohang *et al*., 2018a, p. 12)

The second part of the instrument consists of four items that describe the individuals' privacy concerns of mobile devices. These items are based on previous studies regarding Internet privacy concerns (Hong & Thong, 2013; Koohang *et al*., 2018b). They are modified to reflect the privacy concerns of mobile devices. These items are as follows:

1. I am concerned that my personal information and data are not protected from unauthorized access when using my mobile device in the workplace.
2. I am concerned that unauthorized people may access my personal information and data when using my mobile device in the workplace.
3. When performing a business task on my mobile device in the workplace, I am concerned that I may not have control over my personal information and data.
4. Even when it is necessary to give out information about myself while performing a business activity on my mobile device in the workplace, I am concerned about how my information is collected, processed, and used.

The third part of the instrument contains four items that describe individuals' trusting beliefs about security and data protection of mobile devices. These items are based on a study by Hong & Thong (2013). They were modified by Koohang *et al*. (2018a) to reflect employees' trusting beliefs about security and data protection of mobile devices. These items are as follows:

1. "My company, in general, would be trustworthy in implementing and executing the security and data protection of mobile devices used in the workplace.
2. My company would keep my best interests in mind when dealing with the security and data protection of mobile devices used in the workplace.
3. My company would fulfill its promises related to all aspects of security and data protection of mobile devices used in the workplace.
4. My company, in general, is predictable and consistent regarding the security and data protection for mobile devices used in the workplace." (Koohang *et al*., 2018a, p. 12)

The measuring scale for the instrument was 7 = completely agree, 6 = mostly agree, 5 = somewhat agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, and 1 = completely disagree.

Sample and Data Collection

Approval to administer the instrument to subjects was sought and granted by the Institutional Review Board (IRB) of where this study was originated. Through a professional survey company, we obtained a total of 184 completed surveys from subjects (106 entry-level workers and 78 intermediate-level workers) in various organizations in the USA). The subjects were female (N = 99) and male (N = 85). Their age levels were 21 – 29 (N = 31), 30 – 39 (N = 70), and above 40 (N = 83). Subjects were guaranteed confidentiality and anonymity.

Data Analysis

Prior to answering the research question, we attempt to empirically validate the instrument through the exploratory factor analysis procedure. The procedure first determines the reliability of the data by testing the multivariate normality and sampling adequacy, testing the eigenvalues (Kaiser Criterion), and testing for total % of variance explained for all components. Second, the principal component analysis with varimax rotation is performed to find out how many components with their associated items are retained. Third, Cronbach's alpha is performed to verify the internal consistency among the factors for each component.

Multiple regression analysis (the Enter Method) was used to analyze the data to answer the study's research question. The analysis enters all independent variables in the model regardless of their significant contribution. The analysis shows which of the independent variables (*trusting beliefs and privacy concerns*) can best predict the dependent variable (*security and data protection awareness of mobile devices*). As per Stevens (2001) the multiple regression analysis includes multicollinearity test, the model fit analysis, and the coefficients table to determine the predictor variables (independent variables) that are most influential in predicting the dependent variable. SPSS™ version 25 was used for all data analyses.

RESULTS

First, the result of Kaiser-Meyer-Olkin (KMO = .884), which was well above the threshold of .6 acceptance level indicated the adequacy of sampling. The Bartlett's test of sphericity results (Chi-Squared = 2473.052, df = 120, and p = .000) showed acceptable multivariate normality and sampling adequacy. Second, all criteria for the Kaiser criterion were met, i.e., study subjects were greater than 150 (N = 184), there were less than 30 variables used (18 variables used), and the values of communalities were above .5.

Third, the total variance explained for the three retained components including the initial eigenvalues, the extraction sums of squared loadings, and the rotation sums of squared loadings accounted for 75%, which is greater than the acceptable 70% of the total variability. After the three above tests met the threshold values that indicated the reliability of the data, the principal component analysis with varimax rotation was performed to force the number of components with their associated items/variables to be retained.

Table 2 shows the principal component analysis with Varimax rotation. As can be seen, all three components retained their associated items/variables. Security and data protection awareness of mobile devices retained all its eight items/variables. Privacy concerns of mobile devices retained all its four items/variables. Trusting beliefs about security and data protection of mobile devices retained all its four items/variables. The internal consistency (Cronbach's alpha) for the three components were .91, .93, & .94 respectively.

Table 2: Rotated Component Matrix (N = 184)

	Variables	Components		
		1	2	3
Security and data protection awareness of mobile devices	AWA1	**.701**	.163	.024
	AWA2	**.802**	.205	-.017
	AWA3	**.853**	.183	-.013
	AWA4	**.754**	.298	-.006
	AWA5	**.789**	.065	.014
	AWA6	**.740**	.248	.118
	AWA7	**.810**	.308	-.067
	AWA8	**.711**	.280	-.089
Trusting beliefs about security and data protection of mobile devices	TRUST1	.393	**.820**	-.115
	TRUST2	.214	**.911**	-.103
	TRUST3	.288	**.895**	-.162
	TRUST4	.374	**.791**	-.186
Privacy concerns of mobile devices	PRIV1	-.067	-.122	**.895**
	PRIV2	.012	-.145	**.935**
	PRIV3	.010	-.129	**.929**
	PRIV4	.050	-.049	**.858**

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

Multiple Regression

The multicollinearity test results showed the absence of multicollinearity among the independent variables. The tolerance level for both trusting belief and privacy concerns was .930 which was above .1 acceptance level. The VIF value for both trusting belief and privacy concerns was 1.075.

The Model fit was determined by the values of R, R^2, and R^2_{adj}. These values indicated that the independent variables reasonably predict the dependent variable (R = .591, $R^{2 = .349}$, and $R^2_{adj} = .342$). In addition, the ANOVA showed a significant result indicating a linear relationship between the dependent variable and independent variables ($F_{2, 181}$ = 48.613, p = .000).

The coefficients table (See Table 3) includes the beta weights, t and *p* values for the independent variables. These results determined that both independent variables (trusting belief and privacy concerns) were the predictor variables and that they are most influential in predicting the security of mobile devices.

Table 3: Coefficients Table (N = 184)

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
Model	B	Std. Error	Beta		
(Constant)	.465	.497		.934	.351
Trusting Beliefs	.720	.073	.612	9.842	**.000**
Privacy Concerns	.123	.061	.125	2.017	**.045**

Dependent Variable: Awareness | Predictors: (Constant), Trust, Privacy Concerns

Results of descriptive analysis were as follows. Awareness (X = 4.72, SD = 1.68), Trusting Beliefs (X = 5.34, SD = 1.43), and Privacy Concerns (X = 3.36, SD = 1.72). Results of correlations are shown in Table 4.

Table 4: Correlations (N = 184)

	Awareness	Trusting Beliefs	Privacy Concerns
Awareness	1.000	.579**	-.036
Trusting Beliefs	.579**	1.000	-.264**
Privacy Concerns	-.036	-.264**	1.000

***Correlation is significant at the 0.01 level (1-tailed).*

DISCUSSION

This study was carried out to investigate the variables of success (i.e., privacy concerns and trusting beliefs) in predicting users' security and data protection awareness of mobile devices. Prior to answering the study's research question, we establish the validity and reliability of the instrument with three constructs/components (privacy concerns, trusting beliefs, and security and data protection awareness of mobile devices). Once the instrument was empirically validated, we proceeded to answer the research question. The results of multiple regression analysis indicated that both users' privacy concerns and trusting beliefs were variables of success in predicting the users' security and data protection awareness of mobile devices.

Malhotra *et al*. (2004) stated that privacy concerns can reveal individuals' natural worries about the possible loss of personal information and safeguarding users' privacy is essential in using mobile devices in organizations (Kuo *et al*., 2015). In the meanwhile, users' trust can be lessened with security breaches (Harris & Patten, 2014) and trust is vital to organization's teamwork, productivity, and performance (De Jong, *et al*., 2016). The present study found that users' privacy concerns and trusting beliefs are influential factors in predicting mobile security devices security and data protection awareness. The findings have several implications for practice regarding users' awareness of mobile security devices security and data protection revolving around training and education.

First, privacy and trust are essential while communicating through mobile devices. Security and data protection awareness of mobile devices within organizations must be promoted with training and implementation and execution of policies to improve trust and minimize privacy concerns. Providing mobile security awareness training can potentially increase employees' trust and lessen privacy concerns. Training should be implemented to educate employees on safer mobile security practices which in turn, can help keep organizations more secure.

Second, an area of training that should exist within an organization about privacy is the use of mobile Online Social Network - mOSNs (Krishnamurthy & Willis, 2010). Traditional pieces of personally identifiable information (PII), such as name, age, gender have always been relatively easy to track. With the increased use of mobile devices, user locations are now being exposed even when a user's exact location is not shown. When connecting to mobile OSN's, personal information is being leaked to third-party providers which can then be linked to a user's browsing behavior and potentially reveal their actual identity, thus exposing risk to the user and the company (Krishnamurthy & Wllis, 2010). In training sessions, organizations must include clear and concise instruction on users' browsing behavior to protect personal information which in turn protects organizations' assets.

Third, mobile application vulnerabilities may potentially increase privacy concerns and lessen trust among employees. Training sessions should be implemented within organizations to protect both the user and the organization's assets. Mobile applications offer the ability for users to log in with an existing account. The benefit of this action is a convenience for the user. However, using a social account, for example, to login to another mobile app essentially weakens the security for that account, the app, and the user's place of work. If a social account is hacked, the hacker will then automatically gain access to the apps where the user utilized the same login.

Forth, BYOD may increase a company's risk of a data breach as these devices are (Koohang *et al*., 2017). Training sessions for BYOD is extremely important to ensure adequate security measures for users and organizations. Deshmukh and Wadhe (2012) identified three areas of vulnerability in mobile business operations: lost or stolen devices, unauthorized data access, and gaps in device management and policy enforcement. To mitigate the risk of loss or theft, mobile devices used as a part of a corporate program should follow best security practices that at a minimum requires remote wipe/lock features and user authentication at the device level to include a password, fingerprint or facial recognition to access the content on the device. Organizations allowing employees to BYOD should have a formal policy in place regarding the organization's best practices. The formal policy should be a part of the training sessions and must constantly be communicated to users. Cisco (2014) and Vickerman (2013) stated that areas that should be addressed in the policy include eligibility, allowed devices, device ownership, security and compliance, data ownership, breach investigation procedures, and device support and maintenance procedures. We assert that these areas should not only be a part of the policy manual, but they must be enforced through training sessions and constant communication to safeguard the users and organizations' assets. Furthermore, just like any networked computing system, mobile devices are vulnerable to unauthorized access. Since the employee or other individuals can access corporate data and systems on a personal device outside of the organization's office space, the user has more privacy in which to attempt inappropriate access of the company data. This is where security policy enforcement becomes significant and organizations must support a variety of different mobile device models and platforms.

Fifth, it is impossible to completely mitigate risk when it comes to mobile devices. From a technology perspective, a solution could be not to allow direct installation of corporate applications or data onto an employee's device. Corporate applications can be provided through mobility management software, desktop virtualization, or secure file sharing (Cisco, 2014). Mobility management software can allow an organization to maintain a level of control over devices registered with the system (Pinchot & Paullet, 2015).

Finally, because mobile applications' use has increased significantly (Murtagh, 2014), it is important to educate employees on how to keep their data secure and be mindful of their privacy when using their mobile devices. Organizations must conduct regular and routine training and awareness campaign on mobile app risks.

CONCLUSION

Based on the results of this study, organizations will be better informed on predictors of success in security and data protection awareness of mobile devices, optimizing an understanding of predictors such as trusting beliefs and privacy concerns, thus adding to the mobile security body of knowledge. Limitations of the study include the number of respondents, limited geographic area, and the number of predictor variables. Expanding the response rate and global results would further validate these results, make it generalizable to a global population, and allow for comparison among countries. Additional predictor variables such as leadership, habits, and social factors should also produce interesting results. With mobile device usage at an all-time high, ongoing mobile security research becomes imperative. Future research should study: 1) the impact of training and education on users' security and data protection awareness of mobile technology; 2) security and data protection awareness of mobile devices compared by type of industries and age groups and; 3) additional predictor variables of success that may influence users' security and data protection awareness of mobile devices. Although security concerns will be ongoing, increased knowledge and awareness through research are critical.

REFERENCES

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Arthur, C., & Boggan, S. (2011). Wi-Fi security flaw for smartphones puts your credit cards at risk. *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2011/apr/25/wifi-security-flaw-smartphones-risk.

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

Bapna, R., Gupta, A., Rice, S., Wendell, O., & Sr, H. (2017). Trust and the strength of ties in online social networks: an exploratory field experiment. *MIS Quarterly, 41*(1), 115–130.

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857–869.

Chan, T. Y. (2012). Mobile customer relationship management: Factors affecting consumer mobile technology adoption within the hotel industry. *Studies by Undergraduate Researchers at Guelph, 5*(2), 44-50.

Chiang, H. S. & Tsaur, W. J. (2011). *Identifying smartphone malware using data mining technology*. Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 1-6.

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

Cisco. (2014). Device freedom without compromising the IT network [White Paper]. Retrieved from https://www.scc.com/wp-content/uploads/2015/11/BYOD_White_Paper.pdf

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737-758.

Dai, S., Liu, Y., Wang, T., Wei, T. & Zou, W. (2010), *Behavior-based malware detection on mobile phone*. Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 1-4.

De Jong, BA, Dirks, K.T., & Gillespie, N. (2016). Trust and team performance: A meta-analysis of main effects, moderators, and covariates. *Journal of Applied Psychology, 101*(8), 1134-1150.

Demetriou, S., Merrill, W., Yang, W., Zhang, A., & Gunter, C. A. (2016, February). Free for All! Assessing User Data Exposure to Advertising Libraries on Android. In *NDSS*.

Deshmukh, R., & Wadhe, A. (2012). Mobile security: Why to secure your mobile devices? *International Journal of Advances in Engineering & Technology, III (IV),* 72-74

Felt, A.P., Finifter, M., Chin, E., Hanna, S. & Wagner, D. (2011). *A survey of mobile malware in the wild*. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM).

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information, 8*(2), 42.

Golembiewski, R. T. & McConkie, M. (1975). The centrality of interpersonal trust in group processes. In G. L Cooper (Ed.), *Theories of group processes* (pp. 131-185). London: John Wiley & Sons.

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.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.

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.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

ITIC (2018). Privacy framework. Retrieved February 6, 2019 from https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf

Kim, D. J., Ferrin, D. L., & Rao H. R. (2008). A trust-based consumer decision-making model in electronic commerce; the role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564

Ko, Ch. H., & Jeng S., (2015). Mobile Technology Adopted in Hotel Sales. *The International Journal of Organizational Innovation*, *8*(2), 172-186.

Koohang, A., Floyd, K., Rigole, N., Paliszkiewicz, J. (2018a). Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs. O*nline Journal of Applied Knowledge Management, 6(2), 7-22.*

Koohang, A., Paliszkiewicz, J., & Horn Nord, J. (2018b). Social Media Privacy Concerns Among College Students. *Issues in Information Systems, 19*(1), 11-19.

Koohang, A., Riggio, M., Paliszkiewicz, J. & Nord, J. (2017). Security policies and data protection of mobile devices in the workplace. *Issues in Information Systems*, *18*(1), 11-21.

Krishnamurthy, B. & Willis, C.E. (2010). Privacy leakage in mobile online social networks. In Proceedings of the *3rd Conference on online social networks* (WOSN'10). USENIX Association. Berkely, CA, 4-4

Kuo, K., Talley, P. C., & Ma, C. (2015). A structural model of information privacy concerns toward hospital websites. *Program*, *49*(3), 305-324.

La Polla, M., Martinelli, F., Sgandurra, D. (2013). A survey on security for mobile devices. Communications Surveys & Tutorials, *IEEE*, *15*(1), 446–471.

Leavitt, N. (2011). Mobile security: finally, a serious problem? *Computer*, *44*(6), 11–14.

Lee, C., & Shim, J. (2006). An Empirical Study on User Satisfaction with Mobile Business Applications Use and Hedonism. *Journal of Information Technology Theory and Application*, *8*(3), 57-74.

Lee, Y., & Benbasat, I. (2004). A Framework for the Study of Customer Interface Design for Mobile Commerce, International Journal of Electronic Commerce, *8*(3), 79-102.

Li, Y.-M., & Yeh, Y.-S. (2010). Increasing trust in mobile commerce through design aesthetics. *Computers in Human Behavior*, *26*(4), 673–684.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90.

Lin, J., Lu, Y., Wang, B., & Wei, K. K. (2011). The role of inter-channel trust transfer in establishing mobile commerce trust. *Electronic Commerce Research and Applications*, *10*(6), 615-625.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mallat, N. (2007). Exploring consumer adoption of mobile payments - A qualitative study. *The Journal of Strategic Information Systems*, *16*(4), 413–432.

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

McKnight, D. H. & Webster, J. 2001. Collaborative Insight or Privacy Invasion? Trust Climate as a Lens for Understanding Acceptance of Awareness Systems. In C. L. Cooper, S. Cartwright & P. C. Earley (Eds.) *The International Handbook of Organizational Culture and Climate* (pp. 533-555). Chichester, England: John Wiley & Sons Ltd.

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

Murtagh, R. (2014). *Mobile now exceeds PC: the biggest shift since the internet began*. Retrieved from http://searchenginewatch.com/sew/opinion/2353616/mobile-now-exceeds-pc-the-biggest-shift-since-theinternet-began.

Mylonas A, Kastania A, Gritzalis D. (2013a) Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security, 34*, 47–66.

Mylonas, A.; Gritzalis, D.; Tsoumas, B.; Apostolopoulos, T. (2013b) A qualitative metrics vector for the awareness of smartphone security users. In Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Prague, Czech Republic, 28–29 August 2013; Springer: Berlin/Heidelberg, Germany, pp. 173–184.

Nah, F., Siau, K., & Sheng, H. (2005). The value of mobile applications: a utility company study. *Communications of the ACM*, *48*(2), 85-90.

NIST (2017), Computer Security Resource Center: Glossary. Retrieved March 11, 2019 from https://csrc.nist.gov/glossary/term/information-security-policy

Palen L, Dourish P (2003) Unpacking ‘‘privacy’’ for a networked world. In: CHI’03, pp 129–136, New York, NY, USA, ACM

Paullet, K., & Pinchot, J. (2014). Mobile malware: Coming to a smartphone near you? *Issues in Information Systems*, *15*(2), 116–123.

Pinchot, J., & Paullet, K. (2015). Bring Your Own Device to Work: Benefits, Security Risks and Governance Issues. *Issues in Information Systems*, 16(3), 238-244.

Riegelsberger, J., Angela Sasse, M., & McCarthy, J. D. (2005). Do people trust their eyes more than ears? Media bias in detecting cues of expertise. In: Proceedings of CHI2005. ACM Press, New York, pp. 1745–1748.

Serrano, K. J., Yu, M., Riley, W. T., Patel, V., Hughes, P., Marchesini, K., & Atienza, A. A. (2016). Willingness to exchange health information via mobile devices: Findings from a population-based survey. *Annals of Family Medicine, 14*(1), 34–40.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Sillence E, Briggs P, Harris P, & Fishwick L (2006) A framework for understanding trust factors in web-based health advice. International Journal of Human-Computer Studies, 64(8), 697–713.

Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, *8*(1), 31-41.

Smith, H. J., Dinev, T. & Xu, H. (2011), Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 980-1016.

Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Shin, M. (2012). Secure remote health monitoring with unreliable mobile devices. *Journal of Biomedicine and Biotechnology*. Retrieved March 22, 2019 from https://doi.org/10.1155/2012/546021

Stevens, J. (2001). *Applied multivariate statistics for the social sciences* (4th ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Toch, E. (2014). Crowdsourcing privacy preferences in context-aware applications. *Personal and Ubiquitous Computing, 18*(1), 129-141.

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.

Vance, A., Christophe, E.-D.-C., & Straub, D. W. (2008). Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of Management Information Systems, 24*(4), 73-100.

Vickerman, J. (2013). Bring your own device to work. *Risk Management*, 38-41.

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.

Xu H, Teo HH, Tan BC-Y, Agarwal R (2009) The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems 26*(3), 135-174.

Zhou, T. (2015). Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors. *Information Systems Frontiers, 17*(2), 413-422.