Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 6, issue 2, 2018

Special Issue on Knowledge Management: Research, Organization and Applied Innovation

Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs

Alex Koohang, Middle Georgia State University, GA, USA, alex.koohang@mga.edu

Kevin Floyd, Middle Georgia State Universit, GA, USA, kevin.floyd@mga.edu

Neil Rigole, Middle Georgia State University, GA, USA, neil.rigole@mga.edu

Joanna Paliszkiewicz, Warsaw University of Life Sciences, Poland, joanna_paliszkiewicz@sggw.pl

Abstract

This paper builds a research model to examine the impact of security policy awareness and data protection awareness of mobile devices on employees' trust belief. A survey instrument was administered to a sample in various organizations in the United States (US). Collected data were analyzed using Partial Least Squares - Structural Equation Modeling (PLS-SEM). Results using 222 participants showed that the security policy awareness of mobile devices positively and significantly contributes to employees' trusting beliefs. Likewise, the data protection awareness of mobile devices positively and significantly contributes to employees' trusting beliefs. The findings are discussed.

Keywords: Mobile devices, security awareness, security policy, data protection, and trusting beliefs.

Introduction

The use of mobile devices or mobile technologies in organizations has become increasingly prevalent as employees use them to perform day-to-day organizational tasks (Murtagh, 2014). Forrester Consulting (2012) stated that mobile devices contribute to organizational efficiencies, reduce cycle time, and enhance communication among employees. Furthermore, they offer business values such as improved employee responsiveness, enhanced worker productivity, better customer relations, greater employee/customer satisfaction, reduced inventory, and decreased maintenance costs (Kearns, 2016). Nevertheless, a report by Crowd Research Partners (2017) indicated a significant rise in security threats on mobile devices.

Milligan and Hutcheson (2008) discussed a number of risks and threats associated with mobile devices. Some examples of these attacks and threats are data leakage resulting from device loss or theft, unintentional disclosure of data, phishing attacks, spyware attacks, network-spoofing attacks, and surveillance attacks. Felt, Finifter, Chin, Hanna, and Wagner (2011) stated that malware attacks on mobile devices have greatly increased in the last 15 years. La Polla, Martinelli, and Sgandurra (2013) specified that malware (i.e., worm, Trojan, rootkits, & botnet) is a vicious, hostile, and intrusive software that is written for malicious acts on mobile devices.

Nevertheless, Paullet and Pinchot (2014) stated that most users are not aware of preventive measures that protect their mobile devices against malware.

Malware attacks on mobile devices affect personal, financial, and professional losses. These attacks can lead to impersonation and identity theft (van Cleeff, 2008; Arthur & Boggan, 2011) and have overwhelming concerns for organizations (Liang & Xue,2009). Hogben and Dekker (2010) outlined several threats in mobile devices that can possibly be detrimental to organizational assets. These threats are on personal data, corporate intellectual property, classified information, financial assets, device and service availability/functionality, as well as personal/political reputation.

Many organizations allow employees to use their own mobile devices to conduct business activities. This alternative strategy known as 'bring your own device' (BYOD) is letting employees, business partners, and other users to utilize a smartphone and/or a tablet to perform business activities and access data (Gartner IT Glossary, n.d.). Crowd Research Partners (2017) stated that the key trends influencing enterprise BYOD and mobile security were improved employee mobility, satisfaction, and productivity while security and privacy are the major obstacles of BYOD adoption in organizations. Leavitt (2013) suggested that organizations increasingly demand that employees adhere to certain security procedures while using mobile devices and/or accessing data belonging to the company. However, the chances are that confidential data may be accessed and stored on personal mobile devices.

Statement of the Problem

MobileIron (2014) grouped the security risks and threats of mobile devices into three categories: 1) device-based threats, 2) network-based threats, and 3) user-based threats. To minimize the security risks and threats, the security and the data loss prevention on mobile devices must have a 'layered security approach' that can be implemented using "secure operating system architecture, authentication, remote wipe, encryption, data sharing, network security, application lifecycle management, and secure browsing" (MobileIron, 2014, p. 3).

Even with the implementation of layered security approach for mobile devices, organizations still require having a set of policies and controls for mobile devices. These policies must be communicated to employees through a variety of approaches. Harris, Patten, and Regan (2013) asserted that while organizations integrate mobile technologies to gain business values, they recognize the critical need for implementing security policies and data protection measures for all aspects of mobile devices. Kearns (2016) stated that without sufficient policies and control for mobile devices, organizations could expect the massive threat to their resources. At the same time, it is well know that user trust that brings about confidence and satisfaction among employees can be positively influenced by security policies as well as data protection measures that are set forward by organizations and communicated to employees (Sabel, 1993; Mayer, Davis, & Schoorman, 1995). The breach of data over mobile devices can be upsetting for individuals and organizations. Moreover, organizations can lose user trust if security breaches are experienced (Harris & Patten, 2014).

As mobile devices are increasingly being vulnerable to threats, organizations must address as well as communicate security and data protection issues through formal policies and controls.

The employee awareness of the security and data protection of mobile devices becomes critical because it can minimize threats to valued resources of organizations resulting in a potential increase employees' trust.

Purpose of the Study

The purpose of the present study is to build a research model that examines the impact of 1) the security policy awareness of mobile devices on employees' trusting beliefs and 2) the data protection awareness of mobile devices on employees' trusting beliefs (See Figure 1). Consistent with its purpose, the remainder of the paper is as follows. First, the mobile devices security policy awareness, the mobile devices data protection awareness, and the employees' trusting beliefs are defined. Second, two hypotheses are developed following the methodology that includes the measures, participants, and data analysis. The results are presented, followed by a discussion of findings, implications, limitations, and recommendations for future research.

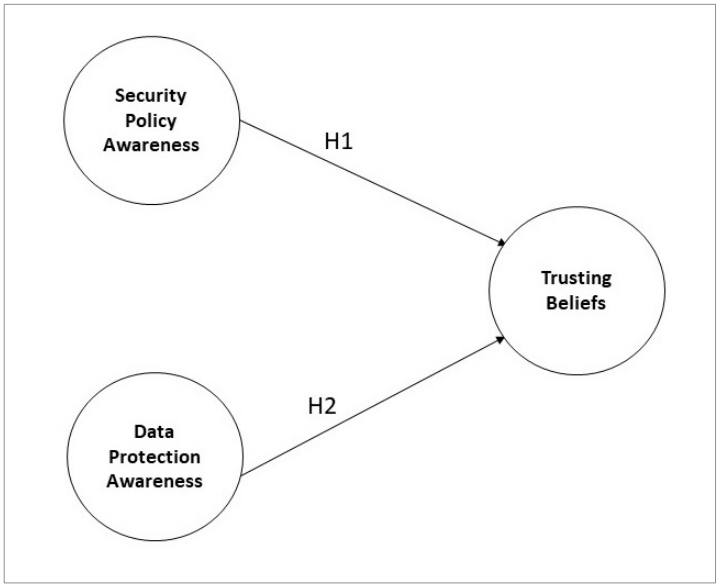

Figure 1. This Study Research Model of Factors Impacting Trusting Beliefs

Definition of Variables

The mobile devices security policy awareness: The knowledge and understanding of policies regarding 1) BYOD, 2) corporate communication conducted on mobile devices, 3) apps used on mobile devices, and 4) disaster recovery plan.

The mobile devices data protection awareness: The knowledge and understanding of 1) organization's deployment of mobile device management (MDM), 2) restrictions on corporate data accessed by mobile devices, 3) enforcing security measures to access sensitive and/or confidential data, and 4) updates of security software to protect data on mobile devices.

The employees trusting beliefs: 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.

Hypotheses Development

Awareness and Trust

In general, awareness promotes and encourages openness and communication among employees (D'Arcy, Hovav, & Galletta, 2009). Increased openness and communication, therefore, builds more trusting climate (Golembiewski & McConkie, 1975). Siponen (2000) defined security awareness as a situation wherein individuals within organizations are aware and committed to the security policies of their organizations. Bulgurcu, Cavusoglu, and Benbasat (2010) defined security awareness as "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (p. 532). Shaw, Chen, Harris, and Huang (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). McKnight and Webster (2001) believed that there is a relationship between awareness and trust. They noted that awareness could reinforce and improve trust because being aware indicates that things are satisfactory within the trusting environment. Furthermore, awareness builds trust between teams, develops trust by enhancing communication within organizations, and promotes openness that contributes to trust within organizations (McKnight & Webster, 2001).

Trusting Beliefs

Trust between parties encourages safe and satisfying relationships. Trust is the confidence between two parties. It is the willingness of one party to engage in interaction with another party that results in benefits and satisfaction for all (Sabel, 1993). There are many classical definitions of trust. For example, trust is:

> "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau, Sitkin, Burt, & Camerer, 1998, p. 395),
>
> "the degree to which the trustor holds a positive attitude toward the trustee's goodwill and reliability in a risky exchange situation" (Das & Tang, 1998, p. 494),
>
> and
>
> "one's expectations, assumptions, or beliefs about the likelihood that another's future actions will be beneficial, favorable, or at least not detrimental to one's interests" (Robinson, 1996, p. 576).

The most widely used dimensions of trust reported in the literature are competence, integrity, benevolence, and predictability (McKnight & Chervany, 1995). The *competence trust* is the ability of a person to accomplish tasks. The *integrity trust* refers to the practice of a set of

standard and acceptable principles. The *benevolence trust* is doing what is in the best interest of people (Paliszkiewicz & Koohang, 2016). McKnight and Chervany (1995) referred to *predictability trust* as being predictable and consistent. The predictability dimension of trust entails being predictable in dealing with the employee; being reliable and dependent in accomplishing tasks, and showing consistency at the workplace.

In this study, we define trusting beliefs as an organization's competence, integrity, benevolence, and predictability in implementing, executing, dealing with, and fulfilling promises related to all aspects of the security and data protection of mobile devices used in the workplace.

Mobile Devices Security Policy Awareness

Koohang, Riggio, Paliszkiewicz, and Nord (2017) identified the top leading issues regarding mobile security policies within organizations. They were 1) BYOD (Ghosh, Gajar, & Rai, 2013; Longo, 2013; Marshall, 2014; Miller, Voas, & Hurlburt, 2012), 2) corporate communication conducted on mobile devices (Goodman, 2004; 2006; He, 2012), 3) mobile apps used in the workplace (He, 2012; Huang, Rau, & Salvendy, 2007; Wu, 2013), and 4) disaster recovery plan (Choo, 2011; Totten & Hammock 2014). We assert that the awareness of these mobile devices security policies is essential to the life of the organization and potentially reduces or eliminates the threats to organizational resources.

Coyle (2001) indicated that the security of mobile devices is an essential key ingredient in building trust within organizations. Employees must feel safe and trust their organizations to implement, execute, and encourage security of mobile devices used in the workplace effectively. Therefore, promoting awareness of mobile devices security policies in the workplace may increase trust among employees. As a result, we state the following hypothesis:

> H1: Security policy awareness of mobile devices positively and significantly contributes to employees' trusting beliefs in organizations.

Mobile Device Data Protection Awareness

Koohang et al. (2017) outlined the top leading mobile data protection issues. These issues were 1) deployment of MDM (Harris & Patten, 2014; Miller et al., 2012; Wu, 2013); 2) restrictions on corporate data accessed by mobile devices (Bankosz & Kerins, 2014; Markelj & Bernik, 2014; Ponemon Institute, 2012), 3) enforcing security measures to access sensitive and/or confidential data (NIST, 2013), and 4) updates of security software to protect data on mobile devices (Martin & Rice, 2011; Wu, 2013). We assert that the awareness of the mobile devices data protection is essential to potentially eliminate detrimental threats to organizational assets. As mentioned earlier, the security of mobile devices depends upon building trust within organizations. Trust creates a safe environment for employees to effectively implement, execute, and encourage security of mobile devices used in the workplace (Coyle, 2001). Therefore, promoting awareness of data protection of mobile devices in the workplace may increase trust among employees. As a result, we state the following hypothesis:

> H2: Data protection awareness of mobile devices within organizations positively and significantly contributes to employees' trusting beliefs in organizations.

Methodology

Measures

We used a seven-point Likert-type instrument comprised of three constructs. The constructs are 1) security policy awareness of mobile devices, 2) data protection awareness of mobile devices, and 3) employees' trusting beliefs. The first two constructs of the instrument are based on a study by Koohang et al. (2017) that studied eight leading issues regarding security policies and data protection strategies of mobile devices within organizations. These two constructs were modified for the present study. The third construct (trusting beliefs) is taken from Hong and Thong (2013), and revised for the present study.

The security policy awareness construct included the following statements:

> SPA1: I am aware that my company has a clear security policy on "bring your own device" (BYOD) in the workplace.
> SPA2: I have sufficient knowledge about my company's security policy regarding corporate communication conducted on mobile devices.
> SPA3: I know that my company has implemented appropriate steps to secure mobile apps I use in the workplace.
> SPA4: I am aware that my company has a clear policy regarding disaster recovery plan in case I experience security breach on mobile devices I use in the workplace.

The data protection awareness construct included the following statements:

> DPA1: I am aware of my company's deployed Mobile Device Management (MDM) that secures, monitors, manages, and supports protection of data on mobile devices.
> DPA2: I know that my company places restrictions on corporate data that may be accessed by employees using their personal mobile devices.
> DPA3: I am aware that my company has a good handle on enforcing security measures to access sensitive and/or confidential data.
> DPA4: I have knowledge about frequent updates of security software on all mobile devices used in the workplace to protect data.

The employees' trusting beliefs construct included the following statements:

> TRUST1: My company, in general, would be trustworthy in implementing and executing the security and data protection of mobile devices used in the workplace.
> TRUST2: My company would keep my best interests in mind when dealing with the security and data protection of mobile devices used in the workplace.
> TRUST3: My company would fulfill its promises related to all aspects of security and data protection of mobile devices used in the workplace.
> TRUST4: My company, in general, is predictable and consistent regarding the security and data protection for mobile devices used in the workplace.

The survey 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, 1 = completely disagree.

Participants and Procedure

The survey instrument was administered electronically via a professional Internet survey site to approximately 1000 participants who working in various organizations in the United States. The participants used mobile devices to conduct business activities in the workplace. Of the 226 returned responses, four were eliminated because of incomplete data yielding a final sample of 222. The subjects were females (56%) and males (44%). Their age category was 21 - 29 (14%), 30 - 39 (19%), and 40 or older (66%). The participants were employed in public (47%) and private (53%) organizations. See Table 1 for additional demographic data.

Table 1. Descriptive Statistics and Demographics of Study Participants (N=222)

BYOD Policy			**Mobile device used to conduct business**		
	Freq.	%		*Freq.*	%
Company Only	66	30%	Smartphone	76	34%
Employee Only	71	32%	Tablet	14	6%
Company & Employee	85	38%	Laptop	82	37%
			Combination	50	23%
Number of employees			**Mobile device operating systems used**		
	Freq.	%		*Freq.*	%
0-250	96	43%	Apple iOS	74	33%
251-500	20	9%	Android	37	17%
501-750	11	5%	Windows	42	19%
751-1000	95	43%	Combination	69	31%

Data Analysis

SmartPLS 3.0, a partial least square structural equation modeling (PLS-SEM) (Ringle, Wende, & Will, 2005) was used to analyze the data. SmartPLS achieves the following:

- Establishing the reliability of the research model by revealing indicator reliability and the internal consistency.
- Establishing the validity of the research model by verifying the convergent validity and the discriminant validity.
- Determining of the structural model to evaluate the R^2 value.
- Determining the acceptance or rejection of the hypotheses by evaluating Path Coefficients, T-Statistics, and P Values.

Results

Establishing the Reliability of the Model

The reliability of the research model was determined by indicator reliability and the internal consistency. Hulland (1999) stated that indicator validity exists if all indicators' outer loadings for each latent variable are 0.70 or higher. Furthermore, the presence of internal consistency requires a value above 0.70 for the composite reliability of each latent variable (Bagozzi & Yi, 1988). As

can be seen in Table 2, all indicators' outer loadings for each latent variable are higher than 0.70, therefore, exhibiting the existence of indicator reliability. Likewise, the values of the composite reliability for each latent variable (Security Policy Awareness = 0.91, Data Protection Awareness = 0.90, & Employees' Trusting Beliefs = 0.95) exceed the threshold value of 0.70, showing the existence of internal consistency.

Table 2. Indicator Reliability and Internal Consistency

		Loadings	Composite Reliability	Cronbach's Alpha	Rho A
Security Policy Awareness	SPA1	0.79	0.91	0.87	0.88
	SPA2	0.89			
	SPA3	0.88			
	SPA4	0.83			
Data Protection Awareness	DPA1	0.80	0.90	0.86	0.87
	DPA2	0.85			
	DPA3	0.90			
	DPA4	0.82			
Employees' Trusting Beliefs	TRUST1	0.90	0.95	0.93	0.94
	TRUST2	0.90			
	TRUST3	0.94			
	TRUST4	0.91			

Establishing the Validity of the Model

The validity of the research model was determined by verifying the convergent validity and the discriminant validity. The convergence validity exists if the average variance extracted (AVE) for each latent variable is 0.50 or higher (Bagozzi & Yi, 1988). The AVE for each latent variable (Security Policy Awareness = 0.72, Data Protection Awareness = 0.71, and Employees' Trusting beliefs = 0.84) was above 0.50 showing the presence of the convergence validity.

Determining the Discriminant Validity

The discriminant validity of the model was determined by assessing the Fornell-Larcker criterion, the cross-loadings of latent variables (Fornell & Larcker, 1981), and the heterotrait-monotrait ratio of correlations (Henseler, Ringle, & Sarstedt, 2015). The Fornell-Larcker criterion requires that the square root of the AVE for each latent variable be higher than its highest correlation with any other latent variables. The cross-loadings of the latent variables must show that an indicator's outer loading on a latent variable is higher than all its cross-loadings with other latent variables. The heterotrait-monotrait ratio of correlations (HTMT) further reveals

a strong discriminant validity if the assessed values for all latent variables are smaller than 0.9. The results for the Fornell-Larcker, the cross-loadings, and the HTMT for the research model showed that all criteria for all three assessments were met. Therefore, the discriminant validity was determined (See Tables 3, 4, & 5).

Table 3. Fornell-Larcker Criterion

	Security Policy Awareness	**Data Protection Awareness**	**Employees' Trusting Beliefs**
Security Policy Awareness	**.85**		
Data Protection Awareness	0.80	**.84**	
Employees' Trusting Beliefs	0.59	0.62	**.92**

Table 4. Cross Loadings

	Security Policy Awareness	**Data Protection Awareness**	**Employees' Trusting Beliefs**
SPA1	**0.79**	0.57	0.43
SPA2	**0.89**	0.69	0.51
SPA3	**0.88**	0.73	0.49
SPA4	**0.83**	0.57	0.43
DPA1	0.67	**0.80**	0.40
DPA2	0.67	**0.85**	0.51
DPA3	0.75	**0.90**	0.60
DPA4	0.63	**0.82**	0.53
TRUST1	0.58	0.59	**0.90**
TRUST2	0.45	0.49	**0.90**
TRUST3	0.52	0.55	**0.94**
TRUST4	0.58	0.60	**0.91**

Table 5. Heterotrait-Monotrait Ratio of Correlations (HTMT)

	Security Policy Awareness	**Data Protection Awareness**	**Employees' Trusting Beliefs**
Security Policy Awareness			
Data Protection Awareness	0.89		
Employees' Trust Beliefs	0.64	0.67	

The Structural Model and Hypotheses Testing Results

The R^2 value for the research model was 0.40, which indicated that the model is strong enough to establish a meaningful interpretation of the data. The standardized path coefficients result and the calculated T-value for determining the acceptance or rejection of the study's hypotheses are presented in Table 6. The first hypothesis (i.e., the security policy awareness of mobile devices positively & significantly contribute to employees' trusting beliefs in organizations) was supported ($\beta = 0.27$, $T = 3.03$, $p = 0.003$). The second hypothesis (i.e., the data protection awareness of mobile devices positively and significantly contribute to employees' trusting beliefs in organizations) was supprted ($\beta = 0.40$, $T = 4.32$, $p < 0.001$).

Table 6. Path Coefficients and T-Values

	Standardized Path Coefficient	**T Value**	**P Value**		**Hypothesis Supported or Rejected**
Security Policy Awareness → Employees' Trust Beliefs	$\beta = 0.27$	3.03	***0.003***	**	Supported
Data Protection Awareness → Employees' Trust Beliefs	$\beta = 0.40$	4.32	***0.000***	***	Supported

* p< 0.05, ** p<0.01, *** p<0.001

Conclusions

The use of mobile technologies within organizations has grown significantly to increase efficiencies and productivity (Murtagh, 2014). This is in large part a result of organizational BYOD policies to support employees' use of mobile devices to perform business activities and to access data (Garner IT Glossary, n.d.). With the increased usage of mobile devices, the need for ensuring that data is protected from rapidly emerging threats is a major priority or organizations. Organizations must promote security policy and data protection awareness of mobile devices to help minimize threats to resources and to increase trust among employees. Research indicates that user trust can be lost if security breaches occur (Harris & Patten, 2014). Employee trust within organizations is an essential component of teamwork, productivity, and performance (De Jong, Dirks, & Gillespie, 2016).

Given the increased use of mobile technologies within organizations and the need for employee trust to promote awareness and productivity, the purpose of this study was to develop a research model that tests the relationship of employee security policy and data protection awareness on employees' trusting beliefs. A sample of 222 participants who used mobile devices to conduct business activities in the workplace was surveyed. The results of this study indicated that there is a significant and positive relationship between security policy awareness of mobile devices and employees' trusting beliefs in organizations. In addition, there is a significant and positive relationship between data protection awareness and employees' trusting beliefs within organizations. Given these findings, it is imperative that leadership in organizations sets effective strategies for security policy awareness and data protection awareness of mobile devices to maintain employee trusting beliefs.

Frenkel (2017) studied the success of security awareness programs and the positive effect of training on employee engagement. The author highlighted the importance of communication as an essential component of successful security awareness programs. This communication includes talking to and engaging with employees. Kodish (2017) explained that organizational trust is a product of communication. Communication must take the form of not only spoken words, but also corresponding actions.

The results of a study conducted by Safa, Solms, and Furnell (2015), revealed that information security knowledge sharing, collaboration, intervention, and experience all have a significant effect on employees' attitudes towards compliance with organizational information security policies. Transparency is recognized as a critical element of knowledge sharing such that increased transparency brings increased awareness, coherence, and comprehensibility to information exchanged between two parties (Pagano & Roell, 1996). Kaptein (2008) explained that transparency is required to ensure that information about organizational conduct can be used by employees to modify or adjust their behaviors. Transparency about the use and protection of data reinforces trust (Morey, Forbath, & Schoop, 2015).

It is clear that the security policy awareness of mobile devices and the data protection awareness of mobile devices positively and significantly contribute to employees' trusting beliefs. Communication and transparency are key elements to promoting awareness of mobile device security and the awareness of mobile device data protection. Communication of awareness can come in many forms. It is important that organizational leadership communicates security policy awareness and data protection awareness through a variety of means, including transparency in shared policy-making, and end-user training programs.

Training, in particular, has been shown to have significant promise with employee security policy awareness and data protection awareness, but how often and when the training is provided should be considered. As suggested by Harris et al. (2013), training programs should be given to new and existing employees at least annually because of the rapid popularity of mobile devices. Combined with the increasing threats to these devices, this need for timely and ongoing training is crucial to increasing awareness and trust. How this training is delivered can also be critical in ensuring employee awareness at a deeper level. For example, in their study on the information richness of security awareness training, Shaw et al. (2009) found that users who participated in richer multimedia-based instruction regarding security awareness did not outperform users who

went through hypermedia-based instruction. Understanding the limitations of certain delivery options can help organizations implement more effective security policy awareness and data protection awareness training, especially when delivered online. Future research is needed to determine the most effective means for communicating data protection awareness and security policy awareness across diverse types of organizations.

This study has limitations that may influence the generalizability of the results. About 66% of the participants in this study were 40 years of age or older. Future studies should use a sample that includes a balance among age categories. Furthermore, this study used a sample of convenience. Future studies may want to use a random sample that may yield different results.

References

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

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

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

Coyle, F. P. (2001). *Wireless Web: A manager's guide.* Boston, MA: Addison Wesley.

Crowd Research Partners (2017). *Mobile security report.* Retrieved from http://crowdresearchpartners.com/portfolio/2017-mobile-security-report/

Das, T., & Teng, B. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review*, *23*(3), 491-512.

De Jong, B. A., 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.

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.

Felt, A., 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*, 3–13.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Forrester Consulting. (2012). *The expanding role of mobility in the workplace*. White Paper, Cambridge MA: Forrester Research, Inc..

Frenkel, K. A. (2017, June 21). Security awareness programs need full-time staff, *CIO Insight*, 1.

Gartner (n.d.). *IT glossary*. Available from http://www.gartner.com/it-glossary/bring-your-own-device-byod/

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.

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, UK: John Wiley & Sons.

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). London, UK: Routledge.

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.

Harris, M. A., Patten, K. P., & Regan, E. (2013). The need for BYOD mobile device security awareness and training. *Proceedings of the Nineteenth Americas Conference on Information Systems,* 1-11.

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

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135.

Hogben, G., & Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency*, *710*(01), 1-61.

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.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal*, *20*(2), 195–204.

Kaptein, M. (2008). Developing and testing a measure for ethical culture of organizations: The corporate ethical virtues model. *Journal of Organizational Behavior, 29*, 923-947.

Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, *8*(1), 36-48.

Kodish, S. (2017). Communicating organizational trust: An exploration of the link between discourse and action. *International Journal of Business Communication*, *54*(4), 347-368.

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.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE communications surveys & tutorials, 15*(1), 446-471.

Leavitt, N. (2013). Today's mobile security requires a new approach. *Computer,* 16–19.

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

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

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

Mayer, R., Davis, J., & Schoorman, F. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709-734.

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,* Chichester, England: John Wiley & Sons Ltd., pp. 533-555.

McKnight, D. H., & Chervany, N. L. (1995, November). Trust building processes in organizational relationships. *Proceedings of the 1995 Decision Sciences Institute,* 751-753.

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

Milligan, P. M., & Hutcheson, D. (2008). Business risks and security assessment for mobile devices. *Information Systems Control Journal, 1*, 24.

MobileIron (2014). Mobile security: Threats and countermeasures. Retrieved from http://www.mobileiron.com/sites/default/files/security/Mobile-Security-Threats-and-Countermeasures-WP-MKT-6361-V1.pdf

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, 93-96.

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

NIST (2013). *Guidelines for managing the security of mobile devices in the enterprise.* Available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Pagano, M., & Roell, A (1996). Transparency and liquidity: A comparison of auction and dealer markets with informed trading. *Journal of Finance*, *2*, 579-611.

Ringle, C., Wende, S., & Will, A. (2005). *SmartPLS 3.0*. Hamburg, Germany: SmartPLS, http://www.smartpls.de/

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students*. Santa Rosa, CA: Informing Science Press.

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

Ponemon Institute (2012). Global study on mobility risks: the United States, available from www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf

Robinson, S. (1996). Trust and breach of the psychological contract. *Administrative Science Quarterly, 41,* 574-590.

Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. (1998). Introduction to special topic forum. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393-404.

Sabel, C. F. (1993). Studied trust: Building new forms of cooperation in a volatile economy. *Human Relations*, *46*(9), 1133-1170.

Safa, N. S., Solms, R. V., & Furnell, S. (2015). Information security policy compliance model in organizations. *Computers and Security, 56,* 70-82.

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.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, *8*(1), 31-41.

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.

van Cleeff, A. (2008). Future consumer mobile phone security: A case study using the data-centric security model. *Information security technical report, 13*(3), 112–117.

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.

Authors' Biographies

Dr. Alex Koohang is Payton Anderson Eminent Scholar, Endowed Chair of Information Technology, Professor, and Dean of the School of Information Technology at Middle Georgia State University. He is the author/co-author of numerous scholarly papers and has written/edited several books. Currently, he is the editor-in-chief of the *Journal of Computer Information Systems* and serves on the editorial review board of several IS/MIS publications. He is a Fellow at the Informing Science Institute. Dr. Koohang is the recipient of many awards, including IACIS Computer Educator of the Year and Lifetime Academic Achievement Award from IIAKM.

Dr. Kevin Floyd is associate dean and professor of information technology at Middle Georgia State University. His teaching interests include web technologies, database design and development, leadership in IT, and research methods. He has published in the areas of cybersecurity, leadership and ethics, and instructional technology. He currently serves as the web administrator for the International Association for Computer Information Systems (IACIS) and is a reviewer and mentor for the National Security Agency (NSA) and the Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CD) program.

Dr. Neil Rigole is an Assistant Professor of Information Technology at Middle Georgia State University where he teaches at both the graduate and undergraduate level. His primary teaching focus is in digital media production and his research focus is in increasing student engagement in online learning via active learning, gamification strategies, and rich media instructional design. Dr. Rigole has over two decades worth of experience teaching and leading initiatives and programs at the state and local level in higher-ed, k12, and adult/technical education.

Dr. Joanna Paliszkiewicz is a specialist in management issues connected with knowledge management, intellectual capital and trust management. She holds the rank of University Professor of Warsaw University of Life Sciences and Polish-Japanese Academy of Information Technology. Prof. J. Paliszkiewicz is well recognized in Poland and abroad with her expertise in management issues. She has published over 170 original papers and eight books. She serves on the editorial board of several international journals. She is the editor in chief of Issues in Information Systems and deputy editor-in-chief of Management and Production Engineering Review Journal. Dr. Paliszkiewicz was named the 2013 Computer Educator of the Year by IACIS.