Journal of the Midwest Association for Information Systems (JMWAIS)

Volume 2019 | Issue 1 Article 2

2019

Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory

Cindy Zhiling Tu
Northwest Missouri State University, cindytu@nwmissouri.edu

Joni Adkins
Northwest Missouri State University, jadkins@nwmissouri.edu

Gary Yu Zhao
Northwest Missouri State University, zhao@nwmissouri.edu

Follow this and additional works at: https://aisel.aisnet.org/jmwais

Recommended Citation
Tu, Cindy Zhiling; Adkins, Joni; and Zhao, Gary Yu (2019) "Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory," *Journal of the Midwest Association for Information Systems (JMWAIS)*: Vol. 2019 : Iss. 1 , Article 2.
DOI: 10.17705/3jmwa.000045
Available at: https://aisel.aisnet.org/jmwais/vol2019/iss1/2

This material is brought to you by the AIS Affiliated and Chapter Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Journal of the Midwest Association for Information Systems (JMWAIS) by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Journal of the Midwest Association for Information Systems

Volume 2019 | Issue 1 Article 2

Date: 01-31-2019

Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory

Cindy Zhiling Tu
Northwest Missouri State University, cindytu@nwmissouri.edu

Joni Adkins
Northwest Missouri State University, jadkins@nwmissouri.edu

Gary Yu Zhao
Northwest Missouri State University, zhao@nwmissouri.edu

Abstract

As security concerns have become critical to organizations' Bring Your Own Device (BYOD) strategy, it is important for employees to comply with organization's security measures and policies. Based on the protection motivation theory, this study develops a theoretical model to identify the key factors that affect an employee's intention to comply with organization's BYOD security policies. This model also enriches general Protection Motivation Theory (PMT) by investigating how unique BYOD features may play moderating roles on the relationships between employee's security perceptions and compliance intention. A survey of organization employees who were using their own devices in their workplace was conducted. The research model was tested using the partial least squares (PLS) approach. The results suggest that employees' threat appraisal and coping appraisal affect their intention to comply with BYOD security policies. Further, mixed usage of device and company surveillance visibility are verified moderators. This study contributes to both academics and management practice.

Keywords: Bring your own devices (BYOD), protection motivation theory, threat appraisal, coping appraisal, moderation.

Please note: A prior version of this article received the Midwest Association for Information Systems (MWAIS) 1st. place best paper award at the MWAIS 2018 conference in St. Louis, MO. The article has been expanded and subject to a second round of reviews. We congratulate the authors.

DOI:1017705/3jmwa.000045
Copyright © 2019 by Cindy Zhiling Tu, Joni Adkins, and Gary Yu Zhao

1. Introduction

With the fast development of mobile technology, Bring Your Own Device (BYOD) has become a generational phenomenon and the trend is still growing. BYOD refers to employees bringing their personally owned mobile devices such as laptops, tablets, and smart phones to the workplace, and using those devices to access privileged company information and applications (Miller, Voas, & Hurlburt, 2012). Industry surveys reveal that 72 percent of corporations allow personal devices to connect to corporate networks (Tenable Network Security, 2016) and 87 percent of companies rely on their employees using personal devices to access business apps (Lazar, 2017). Benefits of BYOD include increased employee satisfaction, productivity and innovation, and cost savings for the company.

While BYOD increases convenience, efficiency, productivity, and flexibility, it also brings a range of new security risks such as device loss, data contamination, and corporate network control issues. First, due to their portability and the fact that individuals are routinely carrying mobile devices with valuable data assets wherever they go, mobile devices are easily lost or stolen. A lost BYOD device can be a real source of concern to organizations, not only because of the cost of hardware itself, but more importantly because of the sensitive personal and organization information it may contain (Tu, Yuan, & Archer, 2014). Second, the combining of personal data and business information on a device poses a great threat to organizations due to the intended or inadvertent disclosure of sensitive data (Miller et al., 2012). Business files downloaded onto a BYOD device may be shared or stored with limited security, thus exposing the organization to the risk of a data breach. In addition, personal files from the mobile device that contain malware may spread to the business or internal file servers and other enterprise assets. Finally, BYOD devices might be located outside of the organization, sometimes connected to an unsecured wireless network. Organizations have less oversight over the users who are connected to their network and less ability to classify the devices and user profiles. As external devices are attached, malware could migrate from the personal device into and over the company networks. Internal email systems may be easily attacked during non-business hours because most of mobile devices lack antivirus software and most email and web traffic accessed remotely bypass inspection by firewalls and gateways (Romer, 2014).

Since BYOD is a developing phenomenon, organizations must fully understand the potential security risk it brings to the organization and that implementing security measures or policies could effectively protect the information security. To protect their mobile content and networks, organizations that opt for BYOD need to use a combination of technical measures and non-technical security policies (Neff, 2013). New technical solutions and best practices for BYOD security are available to organizations, such as mobile device management (MDM), mobile content management (MCM), mobile application manager (MAM), network access control (NAC), desktop/application virtualization, centralized access control and monitoring mechanism, mobile antivirus, enterprise sandbox, and so on (Rivera, George, Peter, Muralidharan, & Khanum, 2013; Romer, 2014). Non-technical security policies can greatly affect the employees' understanding and perception of security issues. BYOD security policies define what devices can be used, what data should be accessed from these devices, what applications and services must be avoided for security and compliance reasons, and what happens when such a device is lost, stolen or the owner leaves the company (Marjanovic, 2013).

It is critical for management and employees to understand the security risks and controls that can minimize or eliminate these risks and the negative impact to the business (Straub, 1990). Due to its unique characteristics, BYOD has introduced new types of risks that made traditional standard security controls inadequate and less effective. Organizations should consider adopting specific technical measures, establishing additional BYOD security policies, and educating employees on how to apply measures and comply with the policies. As security concerns have been critical to organizations' BYOD strategy, it is very important for employees to comply with organization's security measures and policies, both technical and non-technical, to secure the application of BYOD. However, as BYOD devices are usually not corporate-owned, security measures and policies are far less likely to be enforced on personal devices. Individual employees need to take the responsibility for securing their own devices usage. Therefore, it is valuable to study how employees comply with organizational security measures and policies to reduce the BYOD security threat. Prior behavioral research on BYOD security is very limited and little has been done on employees' intentions to comply with organization's BYOD security policies even though such security issues have drawn much attention from practitioners.

This study focuses on individual employee's intention to comply with an organization's security measures and policies to

cope with the BYOD security threat. Based on the protection motivation theory (PMT), we build a research model to investigate the key factors and the specific BYOD features that affect employee's intention to comply with organization's BYOD security policies.

2. Literature Review

To deeply understand BYOD security policy compliance behaviors, we reviewed existing literature on BYOD from four perspectives: BYOD benefits for organizations and employees, security risks from BYOD, security measures and policies for BYOD, and factors affecting employee's compliance intention.

2.1 BYOD Benefits

Organizations can benefit from BYOD for productivity, management flexibility, cost saving, and maximized employee contentment (Olalere, Abdullah, Mahmod, & Abdullah, 2015). A BYOD environment can increase the productivity of employees (Crossler, Long, Loraas, & Trinkle, 2014; Gajar, Ghosh, & Rai, 2013; Ganiyu & Jimoh, 2018; Romer, 2014; Waterfill & Dilworth, 2014; Zahadat, Blessner, Blackburn, & Olson, 2015). BYOD provides employees with a new effective channel for collaborating with colleagues and interacting with customers, therefore improving the productivity of employees (Varbanov, 2014).

BYOD allows employees to work effectively irrespective of their locations (Vignesh & Asha, 2015). Employees enjoy the advantage of increased functionality offered by smartphones and tablet apps (Blizzard, 2015). The flexible BYOD environment attracts more job seekers and it consequently prompts BYOD flexibility (Waterfill & Dilworth, 2014).

BYOD helps organizations save money through reduced mobility cost, fewer devices to purchase, and better utilization of corporate IT resources (Varbanov, 2014). Because BYOD devices are owned by employees, organizations save the cost in mobile devices purchases. Employees maintain their own devices so organizations can provide less IT maintenance or services to the BYOD devices. As less IT help is needed for devices, organizations can utilize its IT resources more efficiently.

When employees can choose their own devices for work, they are happier and more satisfied in work (Waterfill & Dilworth, 2014). BYOD provides an opportunity to bridge the gap between corporate and consumer technologies and solutions (Romer, 2014). Consumer applications are constantly improving towards convenience, comfortable performance, ease of communication and better functionality, turning smartphones and tablets into the preferred devices for fun and work (Olalere et al., 2015). BYOD allows employees to use applications on their own devices that they know and like, thus improving employee contentment.

2.2 BYOD Security Risks

While BYOD brings benefits to both organizations and employees, it also brings security risks to organizations. Literature has identified the most challenging security threats and risks to BYOD, including lack of security features from mobile devices, data leakage in shared media, data contamination because of mixed usage, and new forms of malware targeting mobile devices (Olalere et al., 2015; Romer, 2014; Zahadat et al., 2015). The extra portability of mobile devices poses a great challenge to the security of the device, along with the information on it as they can be very easily lost or stolen (Romer, 2014; Tu et al., 2014). Personal devices may not be sophisticated in terms of security such as anti-virus programs, patches, firmware updates and configuration settings. Malware threats are becoming more sophisticated than the traditional infection from malicious email links and attachments, especially in the domains of online social networks (OSN) and mobile dev ices (Svajcer, 2014). With the increasing use of personal mobile devices and the trending adoption of BYOD practices, security threats have become even more diverse and dreadful (Dang-Pham & Pittayachawan, 2015).

2.3 Security Measures/Policies for BYOD

Scholars have determined that effective security measures and policies are necessary for BYOD. Mobile Device Management (MDM) applications are developed to address some of the challenges associated with mobile devices, including policy management, digital certificates, software distribution, and inventory management, etc. (Gajar et al., 2013). MDM can effectively reduce risks, maintenance costs and the downtime of equipment (Varbanov, 2014). However, it does not completely address the security challenges of BYOD (Olalere et al., 2015). Mobile application management (MAM) focuses on higher-level management of applications and data rather than on firmware and configuration settings; MAM includes software and services that allow users to manage and control the safety of personal mobile devices throughout their

life cycle (Varbanov, 2014). Mobile Content Management (MCM) is a new class of mobile security solution that focuses on securing content, wherever it is located, providing secure software 'containers' which shield confidential data from unauthorized access and malware infection (Romer, 2014).

Different security policy models are discussed in literature. Zahadat et al. (2015) claim that a BYOD security framework as the solution to BYOD security concerns has three pillars: people, policy management, and technology. Ganiyu and Jimoh (2018) define the relationships between the risk factors and the technical security controls which are crucial toward achieving realistic risk evaluation process in BYOD strategy. A multilevel model is developed with three levels of security policies for BYOD: Organizational level, Application level and Device level policies (Vignesh & Asha, 2015). Multi-platform Usable Endpoint Security (MUSES) model is developed as a user-centric tool to securely manage the BYOD environment and enterprise security policies. Appling machine learning and computational intelligence techniques, MUSES system can predict future security incidences produced by BYOD users (de las Cuevas et al., 2015).

Other technical measures are also very important to BYOD security. It is argued that the next generation security BYOD measures should be MDM integrating with the next generation firewalls (Tokuyoshi, 2013). APIs are the center of the BYOD security strategy and it is easier and far more cost efficient to implement BYOD policies at an API level than at the device level (Thielens, 2013).

2.4 BYOD Security Policy Compliance Study

It is important that organizations design effective BYOD security policies and then employees comply with these policies. Some empirical studies have been done to measure how employees comply with the security polices and what factors determine employees' compliance through the lens of the protection motivation theory (PMT) (Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Hovav & Putri, 2016). These studies examine traditional PMT model factors such as threat susceptibility, threat severity, efficacy, perspective effectiveness and cost, and the effects of such factors on individuals' intention to comply or actual compliance behaviors with respect to BYOD policies. In addition to PMT factors, the research also examines the impact of moral intensity and inconsistent ethical tone on BYOD policy compliance (Crossler et al., 2014).

Through literature review, we identified a few gaps. First, few empirical studies on BYOD security can be found. Second, these limited empirical studies applied the traditional PMT model to BYOD context but did not examine the specific BYOD features in their research models. Third, most sample data were collected from survey of university students, which might not well represent BYOD employees. This study attempts to fill these gaps.

3. Research Model and Hypotheses Development

Protection Motivation Theory (PMT) (Rogers, 1975, 1983) argues that a person's coping with a threat is the result of two appraisal processes: process of threat appraisal and process of coping appraisal. It is one of the most powerful explanatory theories predicting individual intentions to take protective actions (Anderson & Agarwal, 2010). Based on PMT, we develop our research model, proposing that an employee's intention to comply with organization's BYOD security policies is affected by employee's threat appraisal and coping appraisal. Some relationships are moderated by specific BYOD features such as surveillance visibility and mixed usage.

Threat appraisal relates to the perceptions of how threatened one feels based on an evaluation of the components of fear appeal (Rogers, 1983). People assess a threat based on their own perception of the severity of the threat, susceptibility to the threat, and its probability of occurrence. The likelihood of an adaptive response increases when perceptions of severity and vulnerability are high, while reducing when any rewards associated with continuing the maladaptive response are expected. Once an employee is conscious of the security threat, he or she will establish beliefs as to the probability of personally experiencing the threat and the seriousness of the threat. Therefore, threat appraisal is shaped by two components: perceived vulnerability which is the individual's estimation of the probability of the threat occurrence, and perceived severity which is the severity of the threat (Johnston & Warkentin, 2010; Liang & Xue, 2009).

In the BYOD context, an employee develops a threat perception when he or she believes that there is a probability that BYOD may bring security risks and the negative consequences of such risks will be severe to both the organization and himself or herself. Perceived vulnerability refers to an employee's subjective probability that BYOD security threats will negatively affect him or her. It is associated with the employee's assessment of his/her probability of being exposed to the unfavorable threat. If an employee perceives that a security threat may occur with damages or disturbances, he or she is more likely to consider complying with organization's BYOD security policies to handle the BYOD security risk. Conversely, if employees do not believe that they are truly confronted by such threats, they are less likely to be concerned. In essence, if an employee perceives the threat to be real and is concerned, the likelihood of compliance with security policies is increased. Previous studies have found this variable's significant effect on the intentions to adopt protective behaviors in different contexts, such as small and medium-sized business (SMB) executives' decision to adopt anti-malware software (Lee and Larsen, 2009), user's security behaviors in personal computer usage (Liang & Xue, 2010), user's coping with mobile device loss and theft (Tu et al., 2014), and user's intention to perform malware avoidance behaviors at a BYOD-enabled university (Dang-Pham & Pittayachawan, 2015). Along the same vein, employees are expected to seriously consider complying with organization's BYOD security policies when they perceive they have a high likelihood of facing security threats. We thus hypothesize:

H1: Perceived vulnerability positively influences employee's intention to comply with BYOD Security Policies.

Perceived severity refers to the extent to which an employee perceives that negative consequences caused by BYOD security risks are severe to the organization and himself/herself. It is expected that the more seriously people perceive the magnitude of the negative consequences resulting from the threat event, they are more likely to adopt recommended adaptive actions. Empirical studies have found that perceived severity exerts a significant effect on the intentions to follow protective actions (Beaudry & Pinsonneault, 2005; Crossler et al., 2014; Lee & Larsen, 2009; Tu, Turel, Yuan, & Archer, 2015). When employees' perceptions of the damage or danger of BYOD security risks increase, they will behave in a more cautious manner and comply with the BYOD security policies. Conversely, when employees perceive that the severity of the risks has diminished, they will behave in a less cautious manner. Hence, we propose the following hypothesis:

H2: Perceived severity positively influences employee's intention to comply with BYOD Security Policies.

Coping appraisal involves perceptions of intrinsic and extrinsic factors available to prevent a threat, as well as perceptions of whether the threat is preventable (Workman, Bommer, & Straub, 2008). The employees need to consider whether the outcome is controllable or not, how confident they feel about adopting the coping behavior, how effectively the coping behavior can prevent the threat, and whether the benefit outweighs the cost of the coping behavior. We propose that three constructs will be appraised in the coping appraisal process: self-efficacy, perceived effectiveness, and perceived cost.

Self-efficacy refers to the employee's self-confidence in his or her ability to perform the coping action (Bandura, 1977, 1982). If people are highly confident in their ability to conduct a recommended action and they do not feel the action is difficult, they are more likely to take the action. With regard to security policy compliance, an individual who believes that he or she has the ability to act in accordance with the policies is likely to have more positive feelings towards the policies and is also more likely to comply with those policies (Herath & Rao, 2010). One empirical study found the higher the users' self-efficacy for the safeguarding measure, the stronger their motivation to avoid IT threats by using the measure (Liang & Xue, 2010). When users believe that they are capable of performing a coping behavior to prevent the loss and theft of mobile devices, they are motivated to take the coping action (Tu et al., 2014). It is also found that, BYOD users' perceptions of self-efficacy have positive impacts on their intentions to perform malware avoidance behaviors (Dang-Pham & Pittayachawan, 2015). Similarly, if employees feel uncomfortable with some technologies and regard it too hard to follow the policies, they will not apply the measures even if they know these measures can manage the security threats. When employees believe that it is not hard for them to follow the BYOD policies and perform coping behaviors, they are motivated to comply with the security policies and implement the security measures. Therefore, we hypothesize that:

H3: Coping action self-efficacy positively influences employee's intention to comply with BYOD Security Policies.

In the context of information security, perceived effectiveness refers to the subjective assessment of a safeguarding measure regarding how effectively it can be applied to avert the security threat (Liang & Xue, 2009). Given the information

about the counteractive measures for coping with the security threats, an employee assesses the effectiveness of the advocated adaptive behavior. In this study, we define perceived effectiveness as an employee's belief that the BYOD security policies will work in averting an undesirable threat of BYOD. It reflects the individual's perception of the objective outcomes produced by complying with the security policies. Prior information security research has found a significant positive impact of perceived effectiveness on adaptive behaviors (Crossler et al., 2014; Hovav & Putri, 2016; Lee & Larsen, 2009; Tu et al., 2014). The more effective the employee perceives the security policies, the more likely the employee will consider them. Hence, we hypothesize:

H4: Perceived effectiveness positively influences employee's intention to comply with BYOD Security Policies.

When employees decide to comply with the security policies, they consider not only the effectiveness, but also the costs. We define perceived cost as an individual's physical and cognitive efforts that are needed to comply with BYOD security policies. Employees consider tangible and intangible costs associated with coping actions, such as money, time, effort, inconvenience, unpleasantness, difficulty, comprehension, and side effects (Lee & Larsen, 2009). Before individuals decide to adopt the recommended action, they often perform a cost-benefit analysis, which may reduce behavioral motivation (Workman et al., 2008). The negative impact of perceived cost on adaptive behaviors has been empirically verified (Lee & Larsen, 2009; Liang & Xue, 2009; Tu et al., 2014). When employees perceive that the cost of complying with security policies outweighs the benefits of protections, they are less likely to enact such practices. We hypothesize that:

H5: Perceived cost negatively influences employee's intention to comply with BYOD Security Policies.

We also expect two unique features of BYOD will play moderating roles on the relationships between employee's security perceptions and compliance intention. Employees are bringing different kinds of devices such as smart phones, tablets, and laptops to work. They may use such mobile devices to access the company's network remotely anytime, anywhere, even via potentially dangerous open WiFi networks. Organizations can hardly monitor who is connecting to the network. Even advanced firewalls or gateways may not be able to detect the mobile attacks. In most BYOD devices, personal data and applications are mixed freely and casually with business information and applications. We define mixed usage as the extent to which personal data and usage are mixed with business information and usage. Surveillance visibility refers to the level of the organization's surveillance and monitoring of remotely accessed users. It can reflect how much the employee is aware of the monitoring from the organization when they use BYOD devices.

Individual's protection motivation stems from both the threat appraisal and the coping appraisal. The threat appraisal assesses the vulnerability of the situation and examines how serious the situation is, while the coping appraisal is how one responds to the situation. The threat appraisal process focuses on the source of the threat (Plotnikoff & Trinh, 2010). In BYOD context, the source of security threat mainly comes from the device itself. Mixed usage and company surveillance may not have much influence on employee's threat appraisal effect. Therefore, we do not investigate the moderation effects of BYOD features on threat appraisal.

The coping appraisal consists of self-efficacy, response efficacy, and the response cost. Coping action self-efficacy is the belief in one's ability, thus the effect of self-efficacy is not affected by device mixed usage or company surveillance. We do not examine the moderation effect on self-efficacy. Response efficacy is the perceived effectiveness of the recommended behavior in removing or preventing possible harm (Prentice-Dunn, Mcmath, & Cramer, 2009). The response cost is the perceived cost associated with the recommended behavior. Response efficacy and cost are related to conducting the coping behaviors, which are influenced by device usage and company surveillance. Therefore, we propose that mixed usage of the device and the surveillance visibility level of the BYOD device may moderate the total effect of perceived effectiveness and perceived cost on compliance intention.

With different levels of mixed usage, employees may assess the effectiveness or cost of their responses to handle BYOD security threats in different levels. If employees seldom use their personal devices for work, they may not think the response effectiveness and the cost of conducting the responses are very important for their intention to comply with security policies.

The more the employees use personal devices for work, the effectiveness of coping behavior becomes more important and the cost is less impeditive for their intention to comply with security policies. Hence, we have the following hypotheses:

H6: Mixed usage positively moderates the positive impact of perceived effectiveness on employee's intention to comply with BYOD Security Policies.

H7: Mixed usage negatively moderates the negative impact of perceived cost on employee's intention to comply with BYOD Security Policies.

When employees are aware that the company is monitoring their BYOD usage, they may assess effectiveness or cost of their responses to cope with BYOD security threats differently. If the employee knows that their usage is not surveilled, they may not care whether the response effectiveness is important or not for them to comply with security policies. Meanwhile, the cost may be a big issue for them to comply with security policies. The effectiveness of coping behavior is more important for an employee's intention to comply with security policies when the company uses more surveillance. Even if the perceived cost of conducting the coping behavior is large, an employee will intend to comply with company policies due to the surveillance visibility. Thus, we hypothesize that:

H8: Surveillance visibility positively moderates the positive impact of perceived effectiveness on employee's intention to comply with BYOD Security Policies.

H9: Surveillance visibility negatively moderates the negative impact of perceived cost on employee's intention to comply with BYOD Security Policies.

The research model is shown in Figure 1.

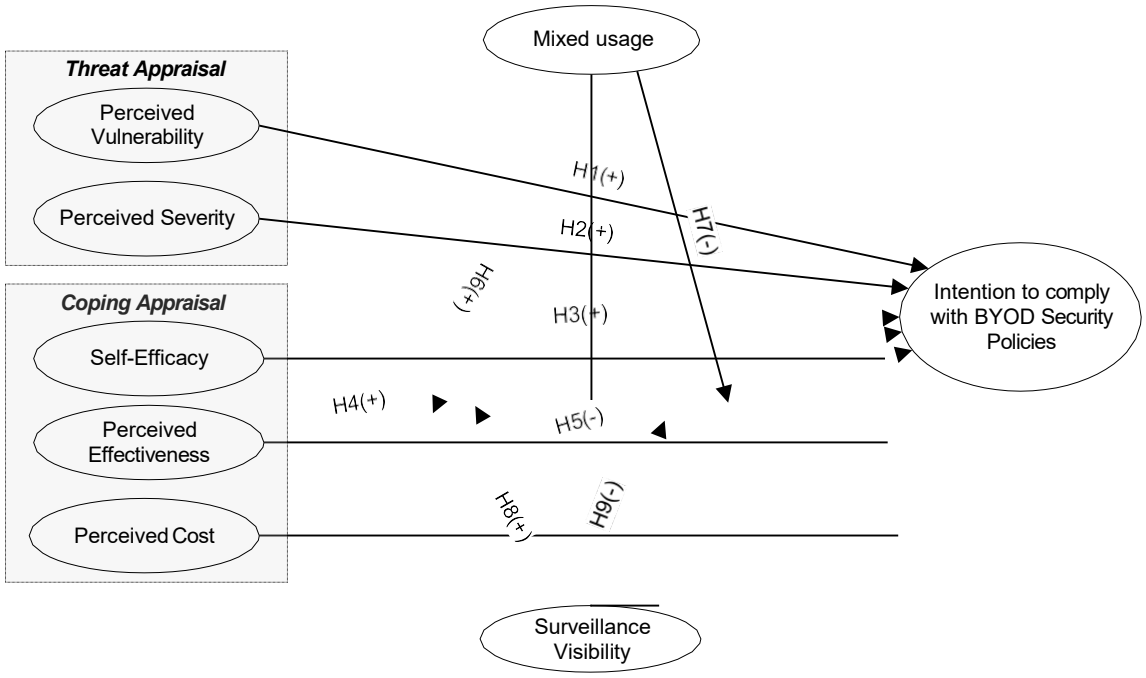


Figure 1. Research Model

4. Research Method and Data Analysis

We conducted an online survey of organization employees who were applying BYOD in their workplace. Participation

was voluntary. We developed all the measurements based on their theoretical meaning and relevant literature. All constructs were measured by multiple items. Except the two moderators, the initial scale items of other constructs were taken from previously validated measures in prior literature and reworded to relate to the BYOD context. The items were scored on a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). Mixed usage and surveillance visibility were tested by one item to examine the levels. All the measurements for each of the constructs are summarized in Appendix A.

A pilot study was conducted to validate the instrument derived from existing scales which were adapted to the context of BYOD security policy compliance. Participants were faculty members and graduate students of a North American university, who had BYOD working experience. A total of 29 responses were obtained. The preliminary consistency and reliability of reflective multi-item scales were first established with Cronbach's alpha scores. The scores for each construct were as follows: intention to comply with BYOD security policies (CI), 0.862; perceived vulnerability (PV), 0.786; perceived severity (PS), 0.795; self-efficacy (SE), 0.771; perceived effectiveness (PE), 0.858; perceived cost (PC), 0.851. These results for Cronbach's alpha for all variables were greater than 0.70, suggesting that the scales of the six reflective constructs were reliable and valid. All items were kept without modification, which retained content validity.

After the pilot study, we employed a commercial survey company (www.surveymonkey.com) to administer our online survey. Participants were recruited randomly among general mobile users whose company had BYOD policies. A usable data set of 122 cases was obtained for testing the theoretical model. It represents a general population of BYOD employees. Most participants had brought several mobile devices to workplace. Sample demographics are provided in Table 1.

Demographic Variable	**Sample Composition**		
		Number	**Percentage**
Gender	Male	65	53.3%
	Female	57	46.7%
Age	18-24	4	3.3%
	25-34	53	43.5%
	35-44	38	31.1%
	45-54	16	13.1%
	55 or above	11	9.0%
Education	High school	15	12.3%
	Bachelor's degree	52	42.6%
	Master's degree	28	23.0%
	Doctoral degree	7	5.7%
	Associate degree	20	16.4%
Country	North America	117	95.9%
	South America	2	1.6%
	Europe	2	1.6%
	Asia	1	0.9%
BYOD device	Laptop or notebook computer	86	89.3%
	Netbook computer (small laptop)	18	14.8%
	Google Chromebook	7	5.7%
	iPad	46	37.7%
	Android tablet	27	22.1%
	Apple iPhone	51	41.8%
	Android smartphone	59	48.4%

Table 1. Demographic Characteristics of the Sample

The research model was assessed using the partial least squares (PLS) techniques with Smart PLS 3.0 (Ringle, Wende, & Becker, 2015) and bootstrapping with 500 resamples (Farivar, Turel, & Yuan, 2017). Analyses were performed to evaluate both the measurement and the structural models.

Descriptive statistics and reliability scores are calculated for all reflective constructs and presented in Table 2 together with the intra-construct correlations. The reliability values of all the constructs are acceptable. The PLS results also indicate an acceptable level of discriminant validity.

Construct	Composite Reliability	Cronbach's Alpha	AVE	PV	PS	SE	PE	PC	CI
PV	0.89	0.81	0.72	**0.85**					
PS	0.85	0.77	0.59	0.72	**0.77**				
SE	0.85	0.74	0.66	0.71	0.71	**0.81**			
PE	0.90	0.86	0.70	0.68	0.68	0.73	**0.81**		
PC	0.92	0.89	0.80	-0.10	-0.04	-0.13	-0.10	**0.89**	
CI	0.87	0.77	0.68	0.76	0.76	0.73	0.68	-0.32	**0.83**

Note: Off diagonal numbers are inter-construct correlations. Diagonal numbers are the square roots of AVE (average variance extracted).

Table 2. Descriptive Statistics and Discriminant Validity

5. Main Findings

The hypotheses were tested by examining the PLS structural model. As shown in Figure 2, the R2 value for CI is 0.76, which means the theoretical model demonstrated substantive explanatory power as 76% of the variance in an employee's intention to comply with BYOD security policies was explained by the model. The significance of all path coefficients was measured. Hypotheses H1 to H5, H6 and H9 were supported.

These results suggest that the more security threats the employees assess when they participate in BYOD, the more intentional they are to comply with BYOD security policies. An individual's threat appraisal consists of perceived vulnerability and perceived severity. The relationship between perceived vulnerability and employee's compliance intention has a statistically significant beta coefficient of 0.18 ($p<0.05$). The single direct effect of perceived severity on employee's security policy compliance intention is more significant with a beta coefficient of 0.26 ($p<0.01$). This implies that employees develop threat perceptions when using BYOD. When they believe that there is probability that BYOD may bring security risks, especially that the negative consequences of such risks may be severe, employees intend to comply with BYOD security policies.

Regarding the impact of employees' coping appraisal, the results reveal that individuals' coping action self-efficacy, perceived effectiveness and perceived cost are all facilitators of their intentions to comply with BYOD security policies. The effect of employee's self-efficacy on his or her policy compliance was statistically significant with beta coefficient of 0.17 ($p<0.05$). Employee's perceived effectiveness also has the significant effect on compliance intention with a beta coefficient of 0.17 ($p<0.05$). When employees are confident in their abilities to follow the security policies and to perform security measures, and when they believe the security policies can effectively avert the security threats, they are intentional to comply with the security policies. Employee's perceived cost is found to have the strongest effect on compliance intention ($\beta= - 0.24$, $p<0.001$). There are tangible and intangible costs associated with an individual's behaviors of following security policies to cope with security threats. When employees believe that the costs of policy compliance are more than the benefits of protection, they are less likely to comply with BYOD security policies.

Among the four moderation hypotheses, two moderations were verified while the other two were not supported. Mixed usage of mobile devices can positively moderate the positive impact of perceived effectiveness on an employee's intention to comply with BYOD security policies. Surveillance visibility negatively moderates the negative impact of perceived cost on employee's intention to comply with BYOD Security Policies.

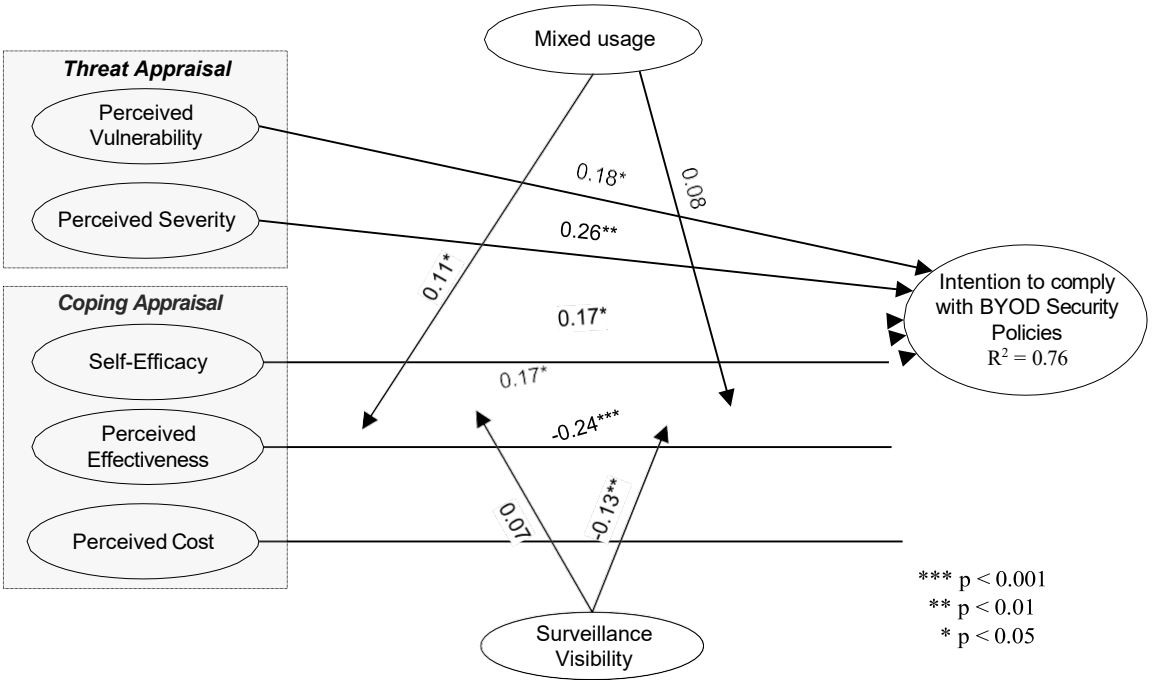
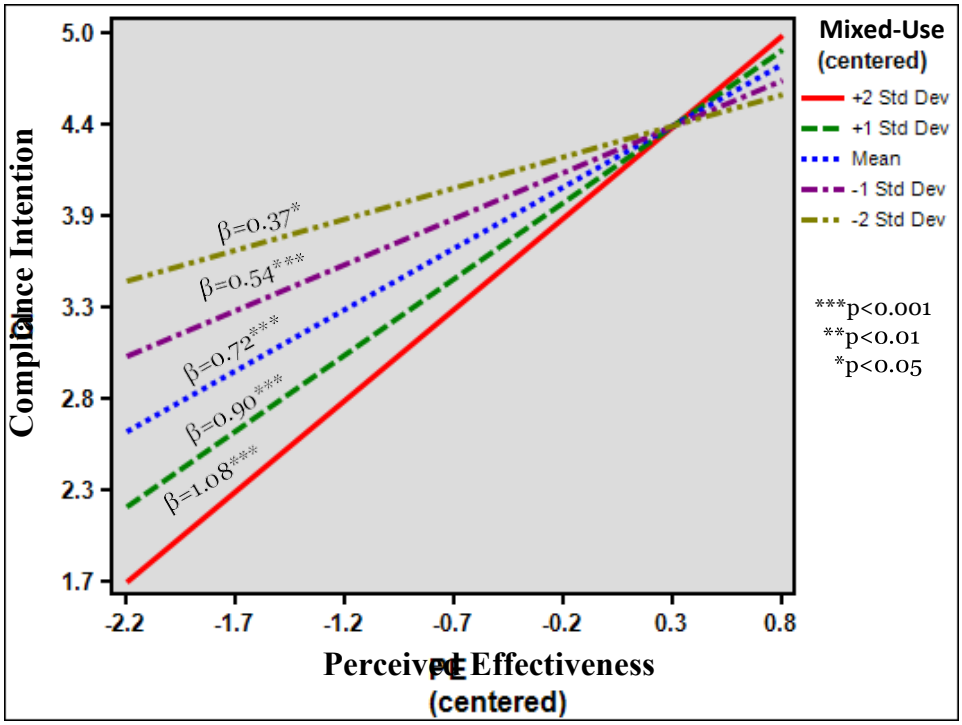


Figure 2. Model Testing Results

We used common moderation plotting techniques (Turel & Bechara, 2017) to illuminate the moderation effects (see Figure 3). In panel A, the slope of the line represents the relationship between compliance intention (CI) and perceived effectiveness (PE). As mixed usage (MU) changes from low (-2 standard deviation) to high (+2 standard deviation), the slope of the line becomes steeper. This means the effect of PE on CI becomes stronger. When employees rarely use their own devices for work (MU -2SD), the effect of PE on CI is the least significant (β=0.37, $p<0.05$). As mixed usage increases, the effect becomes more significant: MU -1SD, β=0.54, $p<0.001$; MU mean, β=0.72, $p<0.001$; MU +1SD, β=0.90, $p<0.001$. When employees use their own device for work the most (MU +2SD), the effect of PE on CI is the most significant (β=1.08, $p<0.001$). It shows that an employee's compliance intention is more influenced byperceived effectiveness when the device is more mixed used. Mixed usage positively drives the relationship between perceived effectiveness and compliance intention.

In panel B, the slope of the line represents the relationship between compliance intention (CI) and perceived cost (PC). As company surveillance (SV) changes from low (-2 standard deviation) to high (+2 standard deviation), the slope of the line becomes flatter. This means the effect of PC on CI becomes less negative (weaker). When employees are least monitored while using their own devices for work (SV -2SD), the negative effect of PC on CI is the most significant (β= -0.27, $p<0.01$). When company surveillance increases, the negative effect becomes less significant: SV -1SD, β= -0.20, $p<0.01$; SV mean, β=-0.13, $p<0.01$; MU +1SD, β=-0.06, not significant. When employees are monitored the most while using their own devices for work (SV +2SD), the effect of PC on CI is not significant at all (β=0.01, ns). It shows that when the BYOD user is more monitored, the user's compliance intention is less affected by perceived cost. Surveillance visibility negatively drives the relationship between perceived cost and compliance intention.

Panel A



Panel B

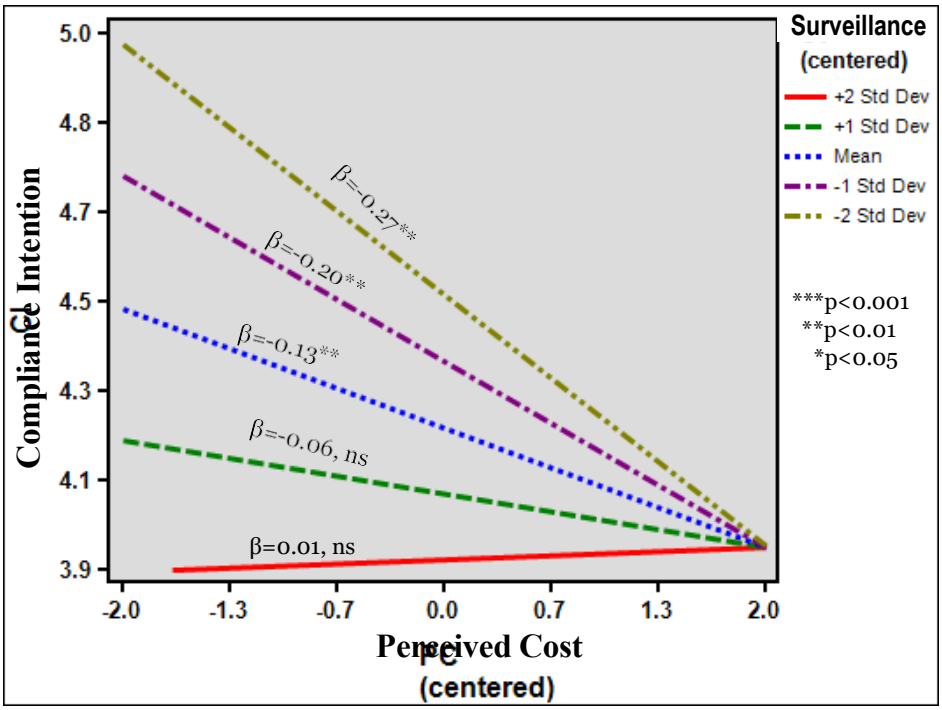


Figure 3. Interaction Plots

6. Discussion and Conclusion

This study empirically investigates the key factors affecting an employee's intention to comply with an organization's BYOD security policies. It also examines the moderation effects of some specific BYOD features on the protection motivation model. The results of the data analyses show that the research model is successful in capturing the main determinants of employee's BYOD policy compliance intention. Employee's compliance intention is significantly affected

by the employee's threat appraisal, which consists of perceived vulnerability and perceived severity, and coping appraisal, which includes self-efficacy, perceived effectiveness, and perceived cost. Two specific BYOD features, mixed usage and surveillance visibility, can influence the effects of employee's coping appraisal on BYOD policy compliance intention. An employee's compliance intention is more influenced by perceived effectiveness when the device is more mixed used with personal data and business information. When a BYOD user is more monitored by the organization, the user's compliance intention is less affected by perceived cost.

This study contributes to information systems (IS) research in several ways. This study develops a theoretical model to identify factors affecting employees' compliance with organization's BYOD security policies, which so far has seldom been empirically studied in the literature. It extends the generalizability of the protection– motivation framework to a relatively unexplored, yet important context, i.e., BYOD security policy compliance. To address this new type of security policy compliance behaviors in BYOD context, new construct measurements are developed according to the unique characteristics of BYOD security risks. The validity and reliability of all the construct measures were empirically verified. The development and validation of the constructs can be useful in future BYOD security studies. Given the prevalence of mobile devices, the BYOD trend and the consequential security threats, research on such security policy compliance behaviors is warranted. Furthermore, this model also enriches general PMT by investigating how unique BYOD features may moderate the relationships between an employee's risk analysis perceptions and his or her intention to adopt BYOD security policies and measures. PMT theory has been adopted in IS research to explain personal protective behavior motivation based on a threat prevention perspective. This study builds a moderation model based on the PMT framework to study the effects of some unique BYOD features on the protection-motivation behaviors. The results provide empirical evidence that two BYOD features can significantly moderate the relationships between an employee's coping appraisal and his or her compliance intention. This study extends the view of PMT employed by past research by adding the new BYOD features.

This study also contributes to management practice. The findings point to several important implications for organizations that apply BYOD practices. First, with the increasing tendency of BYOD, more companies allow their employees to use their own mobile devices to access the organization's systems in order to improve their productivity. Our survey showed that a lot of employees used more than one mobile device for both work and personal usage. BYOD has emerged as a key security risk for organizations. It is therefore important to develop company policies regarding the new security challenges from BYOD applications. Second, the results of this research will help organizations better understand employees' behaviors regarding complying with BYOD security policies. It empirically shows that threat and coping appraisals are important determinants of employees' compliance intentions. Organizations can provide mandatory training or education program to increase their employees' knowledge regarding BYOD security threats and security policies and countermeasures. Organizations can offer incentives and online discussion forums that are devoted to such issues to encourage employees to participate in such training and education programs. Last, the findings of this study indicate that organization's surveillance and monitoring can mitigate the negative effect of employee's perceived cost on compliance intention. If employees are aware of the monitoring from the organization when they use BYOD devices, even when they feel there is cost, they will be more likely to comply with security policies. Therefore, after developing BYOD security policies, organizations should take action to monitor how these policies are implemented and enforced.

Several limitations of this study should be noted. First, our survey participants are mainly from North America, consequently, the generalizability of our findings may be limited. Individuals with different cultures may have different perceptions and thus different motivations. Hence, future research may extend our model and examine the possible effects of cultural factors. Second, we examined only two unique BYOD features in this study. With the fast development of mobile technologies and increasing BYOD applications, there are other BYOD features such as mobility, device variety which may have effects on individual's perceptions and intentions. Future research may investigate more unique BYOD features for their cause effect or moderation effect.

This study seeks to inform behavioral IS security research regarding why employees intend to comply with security policies in the BYOD context. To this end, it builds a moderation model based on PMT framework. The findings depict threat and coping appraisals as determinants of an employee's intention to comply with BYOD policies. Unique BYOD features are found as moderators to the motivation-protection model. Future research is encouraged to further expand this model to help organizations better deploy security policies.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122.

Beaudry, A., & Pinsonneault, A. (2005). Understand user responses to information technology: A coping model of user adaption. *MIS Quarterly, 29*(3), 493-534.

Blizzard, S. (2015). Coming full circle: Are there benefits to BYOD? *Computer Fraud & Security, 2015*(2), 18-20.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security, 48*, 281-297.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–338.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., Garcia-Sanchez, P., & Fernandez-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications, 68*(2015), 83-95.

Farivar, S., Turel, O., & Yuan, Y. (2017). A trust-risk perspective on social commerce use: An examination of the biasing role of habit. *Internet Research, 27*(3), 586-607.

Gajar, P. K., Ghosh, A., & Rai, S. (2013). BYOD: Security risk and mitigating strategies. *Global Research in Computer Science, 4*(4), 62-70.

Ganiyu, S. O., & Jimoh, R. G. (2018). Characterising risk factors and countermeasures for risk evaluation of Bring Your Own Device strategy. *International Journal of Information Security Science, 7*(1), 49-59.

Herath, T., & Rao, H. R. (2010). Protection motivation and deterrence: A framework for securitypolicy compliance in organisations. *European Journal of Information Systems, 18*, 106–125.

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Lazar, M. (2017). BYOD statistics provide snapshot of future. Retrieved from https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

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

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Marjanovic, Z. (2013). *Effectiveness of security controls in BYOD environments*. Retrieved from http://hdl.handle.net/11343/33346

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

Neff, T. (2013). A winning BYOD policy balances usability & control. *Compliance Week, 10*(109), 42.

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of Bring Your Own Device on security issues. *SAGE Open, 5*(2), 1-11.

Plotnikoff, R. C., & Trinh, L. (2010). Protection motivation theory. *Exercise and Sport Sciences Reviews, 38*(2), 91–98.

Prentice-Dunn, S., Mcmath, B., & Cramer, R., 14. (2009). Protection motivation theory and stages of change in sun protective behavior. *Journal of Health Psychology, 14*(2), 297-305.

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. Retrieved from www.smartpls.com (accessed 1 February 2018)

Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). *Analysis of security controls for BYOD (Bring Your Own Device)*. Retrieved from http://hdl.handle.net/11343/33338

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological process in fear appeals and attitude change: A revised theory of protection motivation. In R. Petty (Ed.), *Social Psychophysiology: A Source Book* (pp. 153-176). New York: Guilford Press.

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security, 2014*(1), 13-15.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Svajcer, V. (2014). Sophos mobile security threat report. *In Launched at Mobile World Congress*.

Tenable Network Security. (2016). BYOD and mobile security: 2016 spotlight report results. Retrieved from https://www.tenable.com/blog/byod-and-mobile-security-2016-spotlight-report-results

Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security, 2013*(8), 5-6.

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security, 2013*(4), 12-13.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506-517.

Tu, Z., Yuan, Y., & Archer, N. P. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft. *International Jornal of Mobile Communications, 12*(6), 603-623.

Turel, O., & Bechara, A. (2017). Effects of motor impulsivity and sleep quality on swearing, interpersonally deviant and disadvantageous behaviors on online social networking sites. *Personality and Individual Differences, 108*(2017), 91-97.

Varbanov, R. (2014). Applications of the BYOD concpetion–benefits, risks and approaches. *Business Management, 24*(2), 1-12.

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*(2015), 511-516.

Waterfill, M., & Dilworth, C. (2014). BYOD: Where the employee and enterprise intersect. *Employee Relations Law Journal, 40*(2), 26-36.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. (2015). BYOD security engineering: A framework and its analysis. *Computer & Security, 55*(2015), 81-99.

Appendix A: Measurement Items for Constructs

Construct	Item	Measurement	Source
Intention to comply with BYOD Security Policies (CI)	CI1	I intend to comply with my organization's BYOD policies to protect my own device.	(Davis, 1989; Davis, Bagozzi, & Warshaw, 1989; Tu et al., 2014)
	CI2	I intend to comply with my organization's BYOD policies to protect the confidential data stored in my own device.	
	CI3	I intend to comply with my organization's BYOD policies to prevent unauthorized access to my organization's data, network and internal systems via my own device.	
Perceived Vulnerability (PV)	PV1	There is a good possibility that my organization will have security risks and threats when I use my own device to access organization's confidential data.	(Lee & Larsen, 2009; Huigang Liang & Xue, 2009; Tu et al., 2014)
	PV2	It is extremely likely that my organization will have security risks and threats when I use my own device to access organization's networks.	
	PV3	I feel that my organization will have security risks and threats when I use my own device to access organization's internal systems.	
Perceived Severity (PS)	PS1	If my mobile device is lost or stolen, it will pose a severe security risk to my organization.	(Lee & Larsen, 2009; Huigang Liang & Xue, 2009; Tu et al., 2014)
	PS2	The confidential organization data stored in my own device may be exposed, stolen or unauthorized used by others, thus cause significant loss to my organization.	
	PS3	My remote access to organization's networks and internal systems could be subject to unauthorized access to organization's internal system by cyber criminals.	
	PS4	My mixed use of my own device for both my personal life and work may expose my organization's data and systems to malware.	
Coping Action Self-Efficacy (SE)	SE1	It is easy for me to comply with my organization's BYOD policies and apply all security measures.	(Tu et al., 2014; Workman et al., 2008)
	SE2	I have the capability to comply with my organization's BYOD policies to protect the confidential organization data stored in my own device.	
	SE3	I can apply all required security measures and controls from Endpoint to prevent unauthorized access to my organization's network and internal systems.	

Perceived Effectiveness (PE)	PE1	If I comply with my organization's BYOD policies, my organization will minimize the threat of malware attacks through remote access.	(Tu et al., 2014; Workman et al., 2008)
	PE2	If I comply with my organization's BYOD policies, the confidential organization data stored in my own device will have little chance to be exposed, stolen or unauthorized used by others.	
	PE3	If I comply with my organization's BYOD policies, cyber criminals will have little chance to remotely access my organization's data, network and internal systems.	
	PE4	If I comply with my organization's BYOD policies, my organization's information security will be more protected.	
Perceived Cost (PC)	PC1	I do not comply with my organization's BYOD policies because I do not know how to apply the technical measures.	(Tu et al., 2014; Workman et al., 2008)
	PC2	It is too inconvenient for me to comply with my organization's BYOD policies.	
	PC3	To comply with my organization's BYOD policies will affect my personal usage of my own device.	
Mixed Usage (MU)		The extent to which I use my own device for my work. • I occasionally use my own device for work and do not store organization data in my own device. • I sometimes use my own device for work and store a little organization data in my own device. • I use my own device for work in most time work and store a lot of organization data in my own device. • I fully use my own device for work and store all working data in my own device.	Self-developed
Surveillance Visibility (VI)		The extent to which my organization monitor employees' BYOD usage. • My organization does not monitor employees' BYOD usage at all. • My organization requires employees to safeguard their BYOD usage by themselves, but no formal measures and controls for monitoring. • My organization has some measures and controls to monitor employees' BYOD usage. • My organization has complete measures and controls to monitor employees' BYOD usage	Self-developed

Author Biographies

Dr. Cindy Zhiling Tu is an Assistant professor of Information Systems in the School of Computer Science and Information Systems at Northwest Missouri State University. She received her Ph.D. degree in Information Systems from DeGroote School of Business, McMaster University, Canada. She has published several research papers in professional conference proceedings and in journals such as Information & Management, Information & Computer Security, the International Journal of Mobile Communications, and International Journal of Electronic Commerce. Her research interests are in the areas of information systems security and privacy, mobile commerce, technology acceptance and usage and information systems perceptions.

Dr. Joni Adkins is an Associate professor of Information Systems in the School of Computer Science and Information Systems at Northwest Missouri State University. She received her DBA in Management from Anderson University and her MBA in Management Information Systems from Northwest Missouri State University. She has published articles in the Information Systems Education Journal and the Journal of Higher Education Theory and Practice. Her research interests are in the areas of information systems education, flipped classrooms, BYOD, and use of spreadsheets in decision making.

Mr. Gary Yu Zhao is a graduate student of the School of Computer Science and Information Systems at Northwest Missouri State University. He has rich experience in information system development. His research interests are in the areas of information systems analysis and design, networking and information security, and mobile technology applications.

This page intentionally left blank