5-2018

Complying with BYOD Security Policies: A Moderation Model

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, garyzhao231@gmail.com

Complying with BYOD Security Policies: A Moderation Model

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
garyzhao231@gmail.com

ABSTRACT

Based on the protection motivation theory, this study develops a theoretical model to identify the key factors that affect employee's intention to comply with organization's BYOD security policies. This model also enriches general PMT by investigating how unique BYOD features may play moderating roles on the relationships between employee's security perceptions and compliance intention. A survey on organization employees who were applying BYOD 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's surveillance visibility are verified moderators. This study contributes to both academics and management practice.

Keywords

BYOD, protection motivation theory, threat appraisal, coping appraisal, moderation.

INTRODUCTION

With the fast development of mobile technology, Bring Your Own Device (BYOD) has been 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 workplace, and using those devices to access privileged company information and applications (Miller, Voas and Hurlburt, 2012). Industry surveys reveal that 72 percent of corporations allow personal devices to connect to corporate networks (Tenable Network Security, 2016). A study[1] by the LinkedIn Information Security Community shows that 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 ease of device loss, data contamination, and loss of control to corporate network. 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 and Archer, 2014). Second, the combining of personal data and business information on BYOD device poses a great threat to organizations due to the intended or inadvertent disclosure of sensitive data (Miller et al., 2012). On the one hand, business files downloaded onto a BYOD device may be shared or stored with limited security, thus exposing the organization to the risk of data breach. On the other hand, personal files from the mobile device that contain malware may spread to business or to 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 visibility 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's networks. Internal email systems may be easily attacked

[1] http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf

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 new 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, centralize access control and monitoring mechanism, mobile antivirus, enterprise sandbox, and so on (Rivera, George, Peter, Muralidharan and 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 the 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 the 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, explaining to employees, and educating them to apply measures and to 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 organization's security measures and policies to cope with 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 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.

RESEARCH MODEL

Protection Motivation Theory (PMT) (Rogers, 1983) argues that people's coping with a threat is the result of two appraisal processes: process of threat appraisal and process of coping appraisal. Based on PMT, we develop our research model (see Figure 1). We propose 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 is shaped by two components: perceived vulnerability and perceived severity. The employee develops a threat perception when he or she believes that there is 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. Individuals are expected to seriously consider applying measures and activities to cope with the BYOD security risk when they perceive that they and their organizations have a high likelihood of facing such threat, and at the same time, they perceive that the magnitude of the negative consequences resulting from the threat event is serious.

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 and Straub, 2008). We propose that three constructs will be appraised in the coping appraisal process: perceived effectiveness, perceived cost, and self-efficacy. Perceived effectiveness reflects the individual's perception of the objective outcomes produced by taking the coping actions. The more effectiveness of security policies the employee perceives, the more likely the employee will take them into account. Employees also consider tangible and intangible costs associated with coping actions, such as money, time, effort, inconvenience, unpleasantness, difficulty, comprehension, and side effects (Lee and Larsen, 2009). When employees perceive that costs of complying with security policies outweigh the benefits of protections, they are less likely to enact such practices. Self-efficacy refers to the employee's self-confidence in his or her ability to perform the coping action (Bandura, 1982). When the employee believes that he or she is capable of performing coping measures, he or she is motivated to comply with the security policies and implement the security measures.

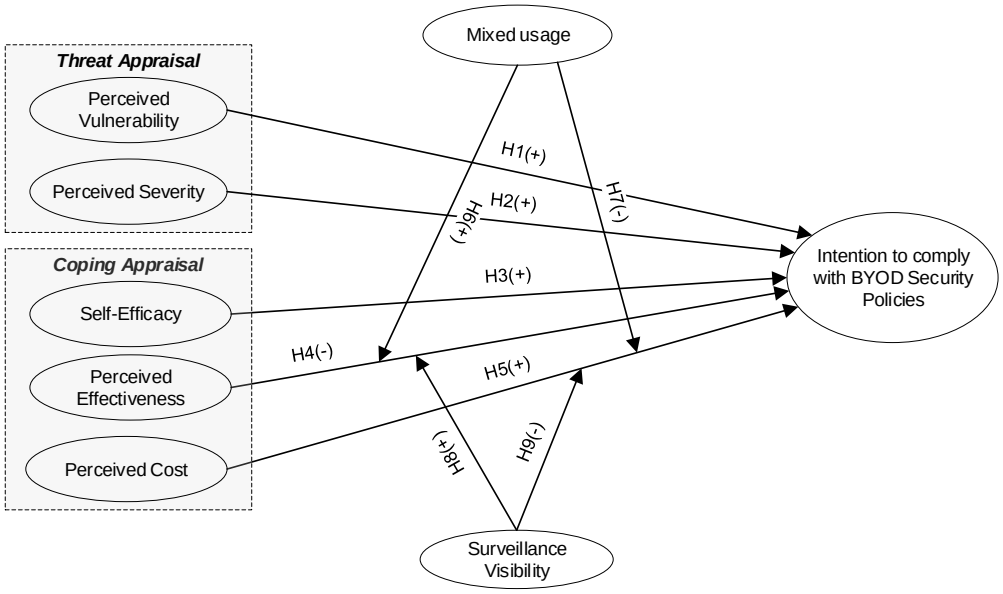

Figure 1. Research Model

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. They may use such mobile devices to access company 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. 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.

Constructs and proposed hypotheses are presented in Table 1.

Constructs	Description	Hypotheses	Relationship
Intention to comply with BYOD Security Policies (CI)	The indication of an employee's readiness to comply with organization's BYOD security policies.		
Perceived Vulnerability (PV)	The extent to which an employee perceives that the BYOD security risks will negatively affect the organization and himself/herself.	H1: PV→CI	+
Perceived Severity (PS)	The extent to which an employee perceives that negative consequences caused by BYOD security risks are severe to the organization and himself/herself.	H2: PS→CI	+
Self-Efficacy (SE)	An employee's self-confidence in his or her ability to comply with organization's BYOD security policies and perform coping measures to prevent BYOD security risks.	H3: SE→CI	+
Perceived Effectiveness (PE)	An employee's belief that compliance with organization's BYOD security policies will work in averting an undesirable threat of BYOD security risks.	H4: PE→CI	+

Perceived Cost (PC)	The extent to which an employee perceives his or her physical and cognitive efforts that are needed to comply with organization's BYOD security policies.	H5: PC→CI	-
Mixed Usage (MU)	The extent to which personal data and usage are mixed with business information and usage.	H6: Moderator to H4	+
		H7: Moderator to H5	-
Surveillance Visibility (VI)	Level of the organization's surveillance and monitoring of remotely accessed users.	H8: Moderator to H4	+
		H9: Moderator to H5	-

Table 1. Constructs and Hypotheses

RESEARCH METHOD AND DATA ANALYSIS

We conducted an online survey on 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. Except the two moderators, all other constructs were measured by multiple items. Wherever possible, initial scale items are taken from previously validated measures in prior literature and reworded to relate to the BYOD context.

A usable data set of 122 cases was obtained for testing the theoretical model. The research model was assessed using the partial least squares (PLS) techniques with Smart PLS 3.0 (Ringle, Wende and Becker, 2015) and bootstrapping with 500 resamples (Farivar, Turel and 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

The hypotheses were tested by examining the PLS structural model. As shown in Figure 2, the R^2 value for CI is 0.76, which means the theoretical model demonstrated substantive explanatory power. The significance of all path coefficients was measured. Hypotheses H1 to H5, H6 and H9 were supported. Among the four moderation hypotheses, two moderations were verified. We used common moderation plotting techniques (Turel and Bechara, 2017) to illuminate the moderation effects (see Figure 3). In panel A, as MU changes from low to high, the slope of the line which represents the relationship between PE and CI becomes more positive (stronger). It shows that employee's compliance intention is more driven by perceived effectiveness when the device is more mixed used. In panel B, as SV increases, the relationship between PC and CI becomes

less negative (weaker). It shows that when BYOD user is more monitored, the user's compliance intention is less affected by perceived cost.

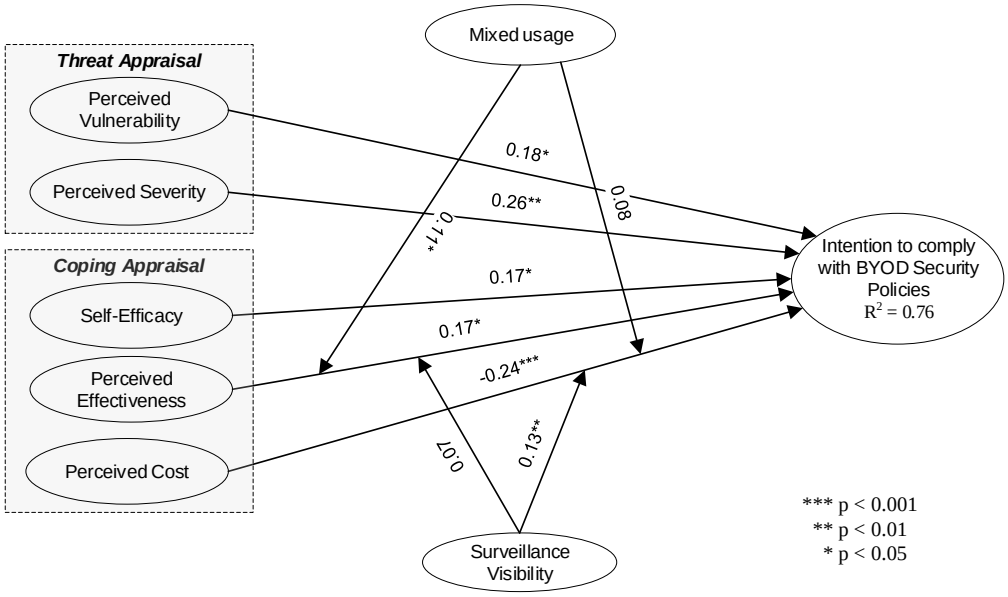

Figure 2. Model Testing Results

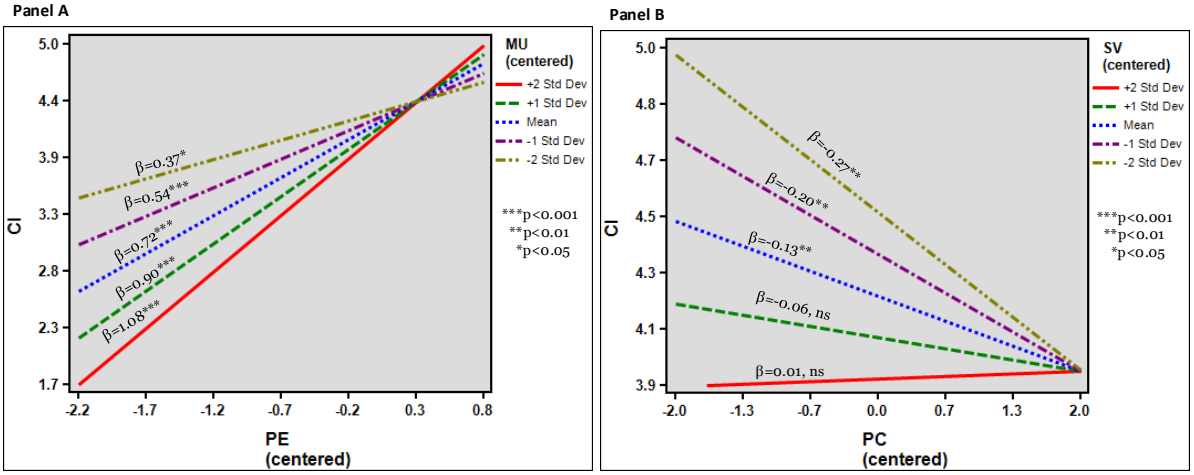

Figure 3. Interaction Plots

CONCLUSION

This study addresses a very important BYOD security issue from individual perspective. It contributes to both academics and management practice. Theoretically, this study proposes 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. This model also enriches general PMT by investigating how unique BYOD features may moderate the relationships between employee's risk analysis perceptions and employee's intention to adopt BYOD security policies and measures. Practically, the results of this research will help organizations better understand employees' behaviors regarding coping with the new security challenges from BYOD applications.

REFERENCES

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

Farivar, S., Turel, O. and 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.

Lee, Y. and 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.

Marjanovic, Z. (2013) Effectiveness of security controls in BYOD environments, The University of Melbourne.

Miller, K. W., Voas, J. and 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.

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

Rivera, D., George, G., Peter, P., Muralidharan, S. and Khanum, S. (2013) Analysis of security controls for BYOD (Bring Your Own Device), The University of Melbourne.

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

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

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

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

Tu, Z., Yuan, Y. and 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. and 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.

Workman, M., Bommer, W. H. and 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.