EMPLOYEES ′ COMPLIANCE WITH BYOD SECURITY POLICY: INSIGHTS FROM REACTANCE, ORGANIZATIONAL JUSTICE, AND PROTECTION MOTIVATION THEORY

Frida Ferdani Putri
Korea University, Seoul, South Korea, fridaferdaniputri@gmail.com

Anat Hovav
Korea University, Seoul, Korea, Republic of, anatzh@korea.ac.kr

Frida Ferdani Putri and Anat Hovav, 2014, "EMPLOYEES ′ COMPLIANCE WITH BYOD SECURITY POLICY: INSIGHTS FROM REACTANCE, ORGANIZATIONAL JUSTICE, AND PROTECTION MOTIVATION THEORY", Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014, ISBN 978-0-9915567-0-0
http://aisel.aisnet.org/ecis2014/proceedings/track16/2

Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory

Complete Research

Putri, Frida, Korea University, Seoul, South Korea, frida_putri@korea.ac.kr

Hovav, Anat, Korea University, Seoul, South Korea, anatzh@korea.ac.kr

Abstract

The trend of bring your own device (BYOD) has been rapidly adopted by organizations. Despite the pros and cons of BYOD adoption, this trend is expected to inevitably keep increasing. Yet, BYOD has raised significant concerns about information system security as employees use their personal devices to access organizational resources. This study aims to examine employees' intention to comply with an organization's IS security policy in the context of BYOD. We derived our research model from reactance, protection motivation and organizational justice theories. The results of this study demonstrate that an employee's perceived response efficacy and perceived justice positively affect an employee's intention to comply with BYOD security policy. Perceived security threat appraisal was found to marginally promote the intention to comply. Conversely, perceived freedom threat due to imposed security policy negatively affects an employee's intention to comply with the security policy. We also found that an employee's perceived cost associated with compliance behavior positively affects an employee's perceptions of threat to an individual freedom. An interesting double-edged sword effect of a security awareness program was confirmed by the results. BYOD security awareness program increases an employee's response efficacy (a positive effect) and response cost (a negative effect). The study also demonstrates the importance of having an IT support team for BYOD, as it increases an employee's response-efficacy and perceived justice.

Keywords:
Information security, Intention to comply, BYOD, Protection motivation, Organizational justice, Reactance theory, Freedom threat

1 Introduction

Bring your own device (BYOD) is defined as an environment that allows employees to use their own personal device to access an organization's resources to perform their work (PricewaterhouseCoopers 2012; Walker-Osborn et al. 2013). Industry reports suggest that organizations adopting BYOD enjoy the benefits in terms of productivity, IT value to business, employee retention, and operation cost (PricewaterhouseCoopers 2012). However, BYOD introduces added risk. Consumer devices are not originally designed for business; they often do not have a sufficient level of security (Durbin 2011). Thus, they are prone to security holes such as malware and data loss (Miller et al. 2012). However, these security risks are not properly addressed by many organizations. A recent information security survey reported that less than 50% of organizations have an information security strategy for BYOD (PricewaterhouseCoopers 2012). Thus, BYOD introduces a new type of insiders' security vulnerability.

Prior literature in information security policy only studied resources that were owned by an organization so that organizations have had full control of their resources. In BYOD, resources are not always owned by the organization. The devices used to perform work are owned by the employees. However, accessed resources are owned by the organization (e.g., network, information). Any attempt to control employees' personal devices could create a perceived threat to their freedom in using their own device. Moreover,

security policy may be perceived as a burden and a hindrance to their work because it restricts the way employees work with their own devices. Despite numerous studies about IS security in an organization, there are no studies that explain IS security compliance in the context of BYOD. This study aims to examine employees' intention to comply with an organization's information system security policy (ISSP) when employees use their personal devices to access organizational resources for work. We use reactance theory, protection motivation theory, and organizational justice theory as the base of analysis of intention to comply. To achieve the objective of this study, this paper attempts to answer the following research questions: What will motivate employees to comply with their organization's BYOD security policy? How does employees' perceived freedom and justice shape their intention to comply with BYOD security policy?

2 Theoretical Background

2.1 Protection Motivation Theory

Protection motivation theory (PMT) was developed by Rogers (1975) to understand fear appeal communication that is intended to influence attitude and behavior change. Fear appeal refers to the communication that describes adverse consequences that happen if one fails to adapt to a communicator's recommendation. The theory held that cognitive appraisal would mediate the effect of fear appeal's components on attitude change by arousing "protection motivation." Protection motivation consists of two processes: threat appraisal and coping appraisal (Maddux and Rogers 1983). Threat appraisal is a process of evaluating maladaptive behavior; it includes a response reward (advantage of maladaptive behavior) and a perception of threat (severity and vulnerability). Coping appraisal is a process evaluating the ability to cope with and remove the threat. This process encompasses response efficacy, self-efficacy, and response costs.

2.2 Reactance Theory

Reactance theory (Brehm 1966) assumes that individuals have a set of free behaviors that are executable. Elimination or a threat of elimination to any free behavior will arouse psychological reactance. Psychological reactance is a motivational state that is directed toward restoration of the threatened or eliminated behavioral freedom. Reactance also refers to the prevention of any further loss of freedom (Brehm 1966; Brehm and Brehm 1981). Freedom restoration can be achieved directly or implicitly. The direct restoration of freedom is achieved by engaging in the threatened or eliminated behavior. Implicit restoration of freedom is achieved by engaging in other behaviors that are considered in the same class as the threatened or eliminated free behaviors. Alternatively, freedom can also be re-established by social implication. That is, another person, who may or may not be under the same threat to freedom, acts in such a way as to remove the threat (Worchel and Brehm 1971).

2.3 Organizational Justice

Organizational justice refers to an individual's fairness perception in organizational context (Greenberg 1987). There are three main types of perceived organization justice: distributive, procedural, and interactional justice (Colquitt et al. 2001). Distributive justice refers to perceived fairness of the outcome (e.g., amount of compensation) that individuals receive (Colquitt et al. 2001; Cropanzano and Ambrose 2001). The most appropriate influence theory to describe distributive justice is equity theory (Adams 1965). Equity theory posits that individuals define fairness based on the ratio of their own perceived outcome (e.g., reward) to their perceived input (e.g., contribution and investment) compared to the corresponding ratio of other individuals, or to themselves in the past. Equity in distributive justice can also be conceived as a mutually beneficial transfer of valued resources between two actors (Cook and Hegtvedt 1983). Over time, equity can be maintained by changes in the value of the resource transfer until an optimum level is achieved (Dansereau et al. 1984 as cited in Scandura 1999). Procedural justice refers to a fairness perception of the means or procedure used to determine the outcome (Thibaut and Walker 1975). Interactional justice, was first introduced by Bies and Moag (1986), deals with

interpersonal treatment by a decision maker during an enactment of a procedure (Bies and Shapiro 1987). Colquitt et al (2001) subdivided interactional justice into interpersonal and informational justice.

3 Bring Your Own Device

BYOD allows employees to use their personal and self-financed device at work to access organizations' resources and use it for work purposes to the same extent as devices offered by the company (Loose et al. 2013). BYOD is well entrenched in companies around the world and is predicted to increase, as reported by Citrix (2011). A recent global survey showed that 42 percent of smart phones and 38 percent of laptops used in the workplace are private devices (Cisco 2012). The BYOD trend is also expected to grow in developing countries, such as Indonesia. According to a survey by the International Data Corporation (as cited in Liputan6 2013), BYOD trend in Indonesia is predicted to increase 52 percent. The respondents said that they planned to increase mobility at work with the use of private mobile devices.

Reference	Research focus	Theory in use
Loose et al. (2013)	The determinants of BYOD service adoption among future employees	Unified Theory of Acceptance and Use of Technology (UTAUT)
Lebek et al. (2013)	Influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices	Theory of reasoned action (TRA) and the technology acceptance model (TAM)
Dernbecher et al. (2013)	Drivers of consumerization behavior	Switching theory
Schalow et al. (2013)	Drivers of using personal media for company purposes	Exploratory study using the methodology recommended by grounded theory.
Niehaves et al. (2013)	Relationship between IT consumerization and employees' work performance	Cognitive model of stress and self-determination theory
Ortbach et al. (2013)	Antecedents of consumerization behavior	Technology acceptance model, technology adoption model, and personal innovativeness

Table 1 Prior studies of BYOD

Security policy is a crucial factor in BYOD environment because employees' activities on their personal devices may affect the overall organization's performance (Stagliano et al. 2013). For example, without proper security protection, employees' personal devices could introduce viruses and malware to the organization's resources as these devices are connected to an organization's network. It is a challenge for organizations to develop BYOD ISSP that balances security and effectiveness with employee empowerment (Mahesh and Hooter 2013). By enacting BYOD ISSP, organizations should be able to control resources that can be accessed by employees and set priority of information to be delivered to employees (Stagliano et al. 2013). Yet, another challenge is to motivate employees to comply with the security policy. György et al. (2012) reported that user non-compliance with security policy is the largest IS security threat in user-driven IT environment. To date, studies in BYOD have focus on the adoption of BYOD and work performance rather than the security challenge of BYOD. Table 1 summarizes a number of existing studies of BYOD.

4 Model Development

4.1 Intention to Comply with BYOD Security Policy

We define intention to comply with BYOD security as one's intention to follow the rules and requirements as defined in the BYOD ISSP when using a personal device for work. An individual's intention has been demonstrated to be a good predictor of an actual behavior (Ajzen 1991). Following the definition in (Bulgurcu et al. 2010), BYOD ISSP can be defined as a statement of employees' roles and responsibilities regarding the use of employees' private mobile devices to access organizational

resources to perform work.

4.2 Threat Appraisal

Threat appraisal is defined as an employee's assessment that a security threat will harm the organization and themselves. In the case of BYOD, it is also reasonable to assume that employees would be unlikely to comply with IS security policy without first discerning security threats (Pahnila et al. 2007). Threat appraisal embodies perceived threat vulnerability and perceived threat severity (Boer and Seydel 1996). Perceived threat vulnerability refers to a perceived chance of a security threat to occur. Perceived threat severity refers to the perceived seriousness of potential impact of the security threat. Many consumers devices used for work are not originally designed for business use. The level of security is relatively low compared to laptop or desktop PC (Durbin 2011). Since employees use the same device for personal and work use, security risk could endanger the organization and the employees' data. For example, without an adequate level of security, a mobile device may be attacked by a *worm*. The *worm* could potentially migrate to the organization's servers and harm the employee's personal data stored in their own device. We posit that if employees believe a security threat is likely to harm their mobile device and organizational computing resources, they are more likely to protect these resources by complying with their organization's security policy regarding BYOD usage. Thus,
H1: Perceived security threat appraisal positively affects an employee's intention to comply with BYOD ISSP.

4.3 Perceived Response Efficacy

Perceived response efficacy is defined as an employee's perception that engaging in compliance behavior will reduce or remove the security threat. In BYOD context, a security threat encompasses a threat to employee's mobile device and the organization's computing resources. Therefore, compliance with an organization's BYOD ISSP would benefit the organization and the employee. One's attitude toward a behavior is determined by the likelihood of the behavior's consequences and the evaluation of those consequences (Fishbein 1963; Fishbein 1961). Therefore, the more desirable the consequences and the higher the probability of those desirable consequences to occur, the more attractive the behavior is (Pligt and De Vries 1998). If there is an increase in one's belief that a desirable outcome will result from a particular behavior, one's intention to perform such behavior will also increase (Maddux et al. 1986; Maddux et al. 1982). Thus, employees would choose to engage in compliance behavior if they believe that such behavior would lead to a positive outcome in response to a perceived security threat (Bulgurcu et al. 2010; Siponen et al. 2007).
H2: Perceived response efficacy positively affects an employee's intention to comply with BYOD ISSP.

4.4 Perceived Digital Mutualism Justice

Perceived digital mutualism justice is defined as a perceived balance of mutual benefit between an employee and the organization subsequent to the enactment of BYOD policy. This definition is derived from the concept of equity in organizational distributive justice, and the mutually beneficial transfer of valued resources between two actors (Cook and Hegtvedt 1983). The perception of justice in this study focuses on the outcome of the fair exchange between an employee and the organization. By using their own devices at their own expense, employees benefit their organization as they become more available and productive (Niehaves et al. 2012). Conversely, employees also need to fulfill their responsibilities in using their personal device according to the organization's BYOD ISSP. Employees would expect a fair reciprocity from the organization based on the contribution that they provide and the cost that they bear. If employees perceive that the organization's reciprocity is not fair, they might try to restore the perception of justice and balance the reciprocity by adjusting their behavior (Cook and Hegtvedt 1983; Walster et al. 1973). For example, an employee might perceive injustice because his contribution to the organization by using his own device for work is reciprocated by restricting him from having full control of that device. Thus, the employee might try to ignore the organization's BYOD rules and thus restore his perceptions of fair exchange. Incompliance with BYOD ISSP could be a means of creating a

disadvantage for the organization as it will increase the organization's vulnerability to security threats (Herath and Rao 2009a; Siponen et al. 2007; Whitman 2004). When employees perceive that organization's reciprocity is fair, they are more likely to comply with BYOD ISSP. Thus,
H3: Perceived digital mutualism justice due to BYOD ISSP positively affects an employee's intention to comply with BYOD ISSP.

4.5 Perceived Freedom Threat

In this study, we define perceived freedom threat as the perceived actual and potential elimination or limitation of an employee's freedom to choose any action on his own device. Interpreting reactance theory in BYOD context, employees may perceive a freedom threat regarding their personal device due to the organization's imposed BYOD ISSP. Employees expect the freedom to do anything they wish with their personal device. However, security policies are likely to impose security tasks or ban particular activities that may restrict an individual's control over their own personal device. For example, IBM has banned applications that allow public file-sharing services on employee-owned devices regardless of whether the use is for personal or work activities (MITTechnologyReview 2012). Such a policy reduces employees' behavioral freedom since the employees may have had this freedom before the ban or at least they are aware that the freedom had existed. A reactance to this enforcement could develop (Brehm and Brehm 1981; Snyder and Wicklund 1976). The aroused reactance would shape employees' counteraction to restore their freedom. Specifically, they may disregard the organization's BYOD policies. We posit that perceived threat to one's freedom would reduce an employee's intention of complying with an organization's BYOD ISSP.
H4: Perceived threat to an individual's freedom negatively affects an employee's intention to comply with BYOD ISSP.

4.6 Perceived Response Cost

Perceived response cost refers to any inconvenience caused by compliance behavior. Perceived response cost relates to both personal and work-related behavior. Bulgurcu et al. (2010) postulated that work impediment caused by compliance with the IS security policy is positively associated with an employee's perceived cost of compliance. An employee's perceived cost related to security compliance behavior may involve an increased physical load (i.e., increasing time and effort to execute a task) and an increased cognitive load. For example, more information or procedure need to be stored and recalled (Beautement et al. 2009). Unlike the security policy for organization-owned resources, employees may perceive complying with BYOD ISSP as more costly because it includes personal cost. A security task is a barrier to an employee's productivity and personal use of the device. For example, installing recommended anti-virus software on an employee's mobile device would cause a regular update request that may interrupt employees from their ongoing work and personal activity. Moreover, installing such software could cause a deceleration of processes executed by the device. Barriers to one's effort to reach an objective could threaten their freedom (Brehm 1966; Brehm and Weinraub 1977). If an individual aims to perform an activity on his device, barriers caused by a security policy could threaten their freedom to complete the activity as expected. Thus, any cost perceived by an employee related to compliance behavior may threaten his perceived freedom. We posit that the higher the perceived cost, the higher is the threat to the individual perceived freedom.
H5: Perceived response cost positively affects an employee's perceived freedom threat.

4.7 Organizational Support

Organizational support in this study refers to the availability of an IT support team to deal with technical issues related to employees' personal devices. Required support provided by an organization reflects the organization's formal attitude toward a particular behavior. Thus, it may signal the probable outcome of the behavior (Compeau and Higgins 1995). In this case, availability of an IT support team could indicate the organization's formal attitude toward security compliance behavior. Therefore, it may affect an employee's perception that complying with BYOD ISSP would result in reduction or removal of security

threat. We posit that availability of organizational support would increase an employee's perceived response efficacy of compliance behavior.
H6a: Organizational BYOD support positively affects an employee's perceived response efficacy in performing BYOD compliance behavior.

The availability of support from an IT team could indicate to employees that an organization is attempting to reciprocate participation in the organization's BYOD program. Employees may view the implementation of adequate security on their devices as a shared responsibility. Furthermore, employees might perceive organizational support as a beneficial resource exchange in return for the use of their own personal devices. Thus, we posit that the reciprocity between employees and the organization is perceived to be more balanced.
H6b: An organization support positively affects an employee's perceived digital mutualism justice regarding BYOD security compliance.

4.8 Security Awareness Program

A security policy needs to be communicated to and understood by employees (Whitman 2004). Thus, it is necessary to have a program that fosters employees' awareness of their rights and responsibilities toward their organization's information assets (Peltier 2005). A security awareness program is developed to highlight the importance of information security and any negative consequences of its failure, and to remind employees of the procedures to follow (Whitman and Mattord 2008). Since a security awareness program conveys the benefit of having security measures in place, it is predicted that BYOD security awareness program will positively influence employees' perception of response efficacy. Bulgurcu et al. (2010) supported this prediction by demonstrating that information security awareness is positively associated with an employee's perception that his information and technology resources at work would be secured if he complied with security policy. Thus, the following hypothesis is proposed:
H7a: Security awareness program positively affects perceived response efficacy of employees' compliance behavior.

We posit that as BYOD security awareness program could make employees become more informed about the procedures they have to perform, their perception of response cost in complying with BYOD ISSP will increase.
H7b: Security awareness program positively affects perceived response cost.

In addition to the core constructs mentioned above, we also controlled for three variables that might influence employees' intention to comply with BYOD ISSP: age, gender, and self-efficacy. Age and gender have been used in IS research related to an individual's security behavioral intention (e.g., D'Arcy et al. 2009; D'Arcy and Hovav 2009; Li et al. 2010; Siponen and Vance 2010; Vance et al. 2012). Self-efficacy is a belief that a person is capable of performing particular tasks (Bandura 1977). In this study, we define self-efficacy as the belief that a person is capable of performing tasks or behaviors related to compliance with BYOD ISSP. Self-efficacy would influence whether one tries to engage in the behavior and the level of effort exerted once the behavior is initiated (Bandura 1977; Bandura 1982). Figure 1 depicts the research model of this study.

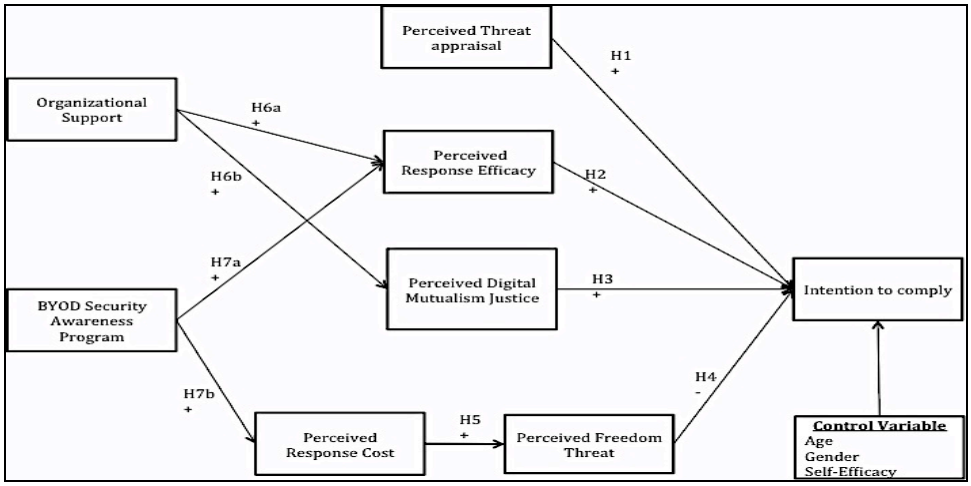

Figure 1 Research Model

5 Methodology

5.1 Development of Measures

To test the above model, we used a survey methodology for data collection. The measurement items of the constructs were primarily adapted from existing scales. Otherwise, new measures were developed by closely following definitions of the constructs (See appendix A for details). Each item involves a 7-point Likert scale to indicate a respondent's level of agreement with the statements in the questionnaire. The survey was originally developed in English, and then translated to Indonesian. The Indonesian version was verified to ensure that both versions have equivalent meaning. Since the study of BYOD compliance is still new in the IS security field, we conducted a preliminary survey prior to the development of our measures. The survey aimed to achieve two goals: (1) obtain insights about the adoption and implementation of BYOD in Indonesia, and (2) determine the prevalent BYOD security policies in organizations. This survey was distributed to employees from various companies. Subsequently, a pilot test was conducted. A few minor and phrase changes were performed based on the result of the pilot test.

Intention to comply with BYOD ISSP (INT_COMP) was measured using a three-item scale from Bulgurcu et al. (2010) and Herath and Rao (2009b). The measurement items of perceived threat appraisal (P_THREAT), perceived response cost (RESP_COST), and perceived response efficacy (RESP_EFF) were adopted from Vance et al. (2012). The measurement of perceived threat appraisal encompasses the items related to perceived vulnerability (PV) and perceived severity of the threat (PS), and also subsumes the items related to personal security threat. Perceived response cost was measured by a six-item scale, which includes the items of work-related and non-work-related cost. Measurement of perceived response efficacy covered items related to reduction of both organizational and personal security threat.

The measurement of perceived freedom threat (FREE_THREAT) used three items adopted from Dillard and Shen (2005). The measured degree of perceived manipulation item is excluded in this study. The measurement of perceived digital mutualism justice (P_JUST) was newly developed for this study by fitting the context of BYOD and reciprocity between an employee and his organization. BYOD security awareness program (SETA) was measured using items scale from D'Arcy et al. (2009), which covers security programs related to both general and specific BYOD security policies. Three specific policies were selected based on our preliminary survey, namely securing personal devices with a password, installing recommended anti-virus, and prohibiting the installation of banned applications. Organizational support (ORG_SUPPORT) was measured by a newly developed scale for this study. This scale measured the availability of technical support for employees who use their personal devices for work. Lastly, self-efficacy (SELF_EFF) was measured using three items from Herath and Rao (2009b).

5.2 Sample and Data Collection

We collected data via a survey from participants in Indonesia. The survey was distributed from August to October 2013. Our potential respondents included those who had been working or are currently working in companies that allow employees to use personal devices for work. We contacted approximately 600 employees from 20 companies. The initial response rate was 55%. The data was further filtered to include only employees working in companies that have a BYOD ISSP. The final sample size for analysis is 230.

6 Analysis and Results

6.1 Measurement Model

A construct should measure the same unique underlying concept in order to ensure the homogeneity and unidimensionality (Winquist and Larson 1998). The composite reliability statistic is considered to be a better indicator of the unidimensionality of a block than the Cronbach's alpha (Chin 1998). The composite reliability values of 0.6 are regarded as acceptable level (Bagozzi and Yi 1988). Convergent validity was assessed by extracting the average variance extracted (AVE) (MacKenzie et al. 2005). An AVE score of 0.5 is commonly acceptable and a score of 0.7 is recommended for a reliable construct (Fornell and Larcker 1981). Table 2 describes the quality of all first order constructs. Composite reliability and AVE values of all constructs exceed the minimum acceptable level, and thus demonstrating appropriate reliability and convergent validity of all constructs.

	Original Number of Items	Items Deleted	AVE	Composite Reliability	Cronbach's Alpha
INT_COMP	7	0	0.713	0.946	0.933
FREE_THREAT	3	1	0.666	0.793	0.582
ORG_SUPP	4	0	0.760	0.927	0.893
PS	6	2	0.695	0.901	0.853
PV	4	1	0.726	0.888	0.811
P_JUST	4	0	0.791	0.938	0.912
RESP_COST	6	0	0.790	0.958	0.947
RESP_EFF	6	0	0.620	0.907	0.880
SETA	8	0	0.749	0.960	0.952

Table 2 Qualities of the First Order Constructs

Discriminant validity is verified if the square root of AVE for each construct is larger than the correlation of the construct with any other constructs in the model (Fornell and Larcker 1981). Table 3 demonstrates that square root of AVE for each construct is larger than the correlation of the construct with any other constructs in the model. In addition, discriminant validity can also be assessed by examining the cross-loadings matrix (Chin 1998). All items have higher loadings with their respective construct than with any other constructs.

	1	2	3	4	5	6	7	8
FREE_THREAT	**0.816**							
INT_COMP	-0.082	**0.845**						
ORG_SUPP	0.043	0.373	**0.872**					
P_JUST	0.102	0.520	0.549	**0.833**				
P_THREAT	-0.027	0.460	0.194	0.179	**0.829**			
RESP_COST	0.393	-0.079	0.100	0.193	-0.334	**0.889**		
RESP_EFF	0.113	0.599	0.351	0.448	0.622	-0.184	**0.788**	
SETA	0.186	0.375	0.599	0.587	0.202	0.268	0.357	**0.865**

Table 3 Inter-construct correlations
The bold numbers on the diagonal are the square roots of the AVE

Perceived threat appraisal (P_THREAT) was measured as a reflective second-order constructs with perceived threat vulnerability (PV) and perceived threat severity (PS) as the first-order constructs. The first-order factors are expected to be distinct but highly correlated because they share the same underlying theme (Dabholkar et al. 1995). In addition, the loadings of the first-order latent variables on the second-order factors have to be equal to or greater than 0.8 (Wetzels et al. 2009). The correlation between PS and PV is 0.829. The loadings of PS and PV on P_THREAT exceed 0.8 (0.967 and 0.945 respectively) and are significant at $p<0.001$. For second-order latent constructs with reflective indicators, AVE could be calculated by averaging the squared multiple correlations for the first-order sub-dimensions (MacKenzie et al. 2011). Values greater than 0.50 indicate that, on average a majority of the variance in the first-order constructs is shared with the second-order construct. AVE of P_THREAT is 0.687, which exceeds the suggested value.

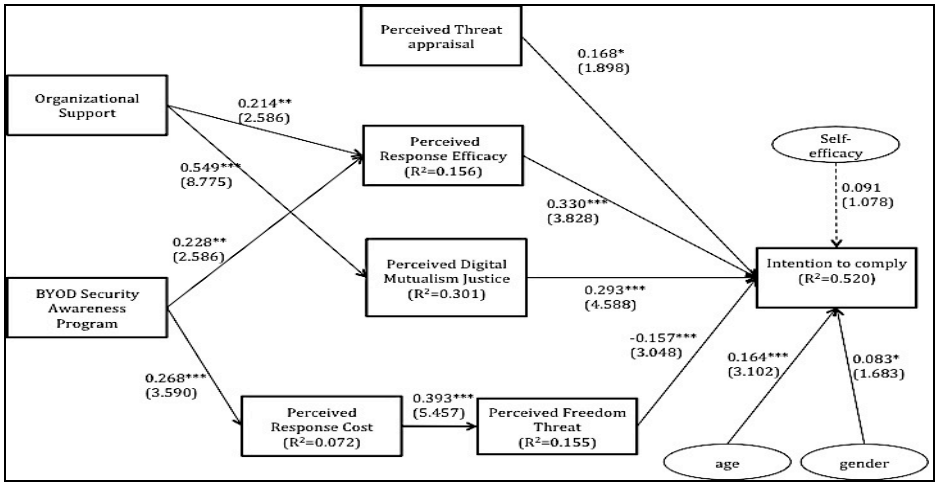

Figure 2 Result of Structural Model (p<0.1; ** p<0.05; *** p<0.01)*

6.2 Structural Model

The analysis results for the structural model are shown in Figure 2. Total variance in intention to comply explained by this model is 52.02%. As predicted, perceived threat appraisal, perceived response efficacy, and perceived digital mutualism justice positively affect intention to comply with BYOD ISSP. On the other hand, perceived freedom threat negatively affects intention to comply with BYOD ISSP. Perceived cost in engaging in compliance behavior was found to positively affect perceived freedom threat. Organizational support was found to positively affect an employee's perceived response efficacy and perceived digital mutualism justice. Lastly, security awareness program related to BYOD positively affects an employee's perceived response cost in engaging in compliance behavior and perceived response efficacy. We found support for all hypotheses, except H1, which was only marginally supported. The relationship between P_THREAT and INT_COMP was only significant at $p<0.1$ (t-value=1.898).

Age was found to have significant effect on intention to comply with BYOD ISSP. Gender's effect is positive but on marginally significant at $p<0.1$. Meanwhile, we did not find significant impact of self-efficacy on intention to comply.

7 Discussion

The results of this study provide support to our research model. Consistent with prior literature, we found that perceived response efficacy positively affect intention to comply. We included items related to efficacy in removing/reducing personal security threat and organizational security threat when we measured perceived response efficacy. During the factor analysis, we found that all items loaded to the same factor. Similarly, we also found that perceived personal security threat and perceived organizational security threat loaded to the same perceived threat factor. The blurring boundaries between work-related and personal use on a single device (Schalow et al. 2013) might be a plausible explanation of these results. As employees use their personal devices for work and personal purpose, they might regard any security threat to be harmful for themselves and the organization. Likewise, if one believes that compliance behavior will reduce/remove personal security threat, she will also believe that the same behavior will be effective in removing organizational security threats and vice versa.

We only got marginal support for the hypothesized relationship between perceived threat appraisal and intention to comply (significant at $p<0.1$). Information security awareness levels in Indonesia are generally low as indicated by the limited government ICT protection regulations and policies (Setiadi et al. 2012). Therefore, people probably would not discern security risks as threats that they need to cope with. Vance et al. (2012) separated the threat appraisal into two constructs and found that perceived severity had significant influence on intention to comply with ISSP but perceived vulnerability did not have significant influence. In this study, we defined a second-order construct of perceived threat appraisal. The use of higher-order constructs is argued to provide more theoretical parsimony and reduce model complexity (Edwards 2001). Furthermore, perceived threat vulnerability and perceived threat are two different variables of threat appraisal in PMT theory (Milne et al. 2000). Thus, it is theoretically reasonable to model perceived threat appraisal as a second-order construct. We performed an additional analysis by using only first-order constructs of perceived threat appraisal. PV and PS were modeled to have direct relationships with intention to comply. We found that perceived threat vulnerability had significant positive effect ($\beta=0.196$, $t= 2.219$) and perceived threat severity had non-significant negative effect on intention to comply ($\beta=-0.021$, $t= 0.227$). These findings are contradictory to Vance et al. (2012) Vance et al (2012) but support Ifinedo (2012). The conflicting results may be due to cultural differences. Ifinedo (2012) collected data in Canada, Vance et al. (2012) collected data in Finland. Cultural variance regarding severity and certainly were previously reported by Hovav and D'Arcy (2012); while in the U.S. severity of punishment reduces misuse intention, in Korea, it has no effect. Conversely, certainty of punishment influences misuse intention in Korea but has no effect in the U.S. Further research is needed to understand the influence of culture on threat perceptions.

We found that perceived digital mutualism justice to positively affect the intention to comply with BYOD ISSP. Benefit transferred between an employee and the organization would shape normative expectations. As the normative expectations regarding implementation of BYOD are met, an employee is more likely to comply with BYOD ISSP. This result provides a useful insight for future studies as suggested by Willison and Warkentin (2013) about how employees' perceived justice influence their security behavior. We carefully defined perceived justice in this study to be specific to BYOD context rather than general justice perception of the organization as a whole. This study also demonstrates that the availability of a technical support team promotes employees' perception of justice. IT support team related to BYOD implementation could be regarded as a formal form of organization's responsibility in implementing BYOD, while employees are responsible to follow the rules stipulated in the BYOD ISSP. Similarly, the availability of an IT support team was also found to positively affect an employee's belief that engaging with compliance behavior would reduce or remove security threat.

The inclusion of perceived freedom threat was new to security policy compliance research. Yet, it fits the BYOD context well. We found that perceived threat to an individual's freedom negatively affects an employee's intention to comply with BYOD ISSP. Reduction of compliance intention is a counteraction to restore the freedom that has been threatened or eliminated due to BYOD ISSP. Consistent to our

hypothesis, perceived response cost was found to increase perceived freedom threat. We found that items related to personal and work-related costs loaded on the same factor. In addition to blurring boundaries between work-related and personal use, we suspect that cultural characteristics explain this specific finding. Indonesia is a collectivist society (Ariyanto et al. 2006; Hofstede 1983; Murphy-Berman and Berman 2002). People in collectivist societies tend to subsume their personal interests under group's interests (Bochner and Hesketh 1994). Thus, a barrier to one's interest and group's interest might be perceived under the same category of cost.

We also found that BYOD security awareness program could be a double-edged sword. Interestingly, BYOD security awareness program increases both perceived response efficacy and perceived response cost. On one hand, a security awareness program briefs and educates employees on how compliance with security policy could reduce security threat. On the other hand, the same program highlights the procedures to follow in order to secure employees' personal devices. Consequently, it may increase an employee's cost perceptions. The effect of SETA on ISSP merits further investigation.

8 Limitations, Contributions and Future Research

This study provides theoretical contributions and practical implications. To the best of our knowledge, this study is the first to examine employees' intention to comply with organizations' ISSP in the context of BYOD. Thus, this study enriches the information security literature by elucidating a contextual perspective. Second, the study highlights the motivators and inhibitors to compliance when the resources in question are personally owned. Specifically, while PMT partially enhances compliance, perceived loss of freedom reduces intention to comply with BYOD ISSP. Similarly, perceptions of justice increase compliance with BYOD ISSP. Therefore, our study contributes in developing more nuanced knowledge of security behavior from a freedom and justice standpoints. Prior research suggests that SETA deters misuse intention. Our results suggest that SETA has a dual role in influencing compliance. This study also draws attention to potential measures related to justice perceptions in the IS security domain.

The result of this study will offer important practical implications for information security practitioners. Organizations that adopt BYOD could understand the factors that may promote employees' intention to comply with organizations' BYOD ISSP. Organizations might need to carefully develop or revisit their BYOD security. We also highlighted the importance of having technical support to assist employees who use personal devices for work. Lastly, this study provides a useful insight to practitioners by demonstrating that a security awareness program specific to BYOD would have both advantages and adverse impact. It is advisable to refine the strategy of BYOD security awareness programs by taking this finding into consideration.

The present study has several shortcomings. In calling attention to the potential limitations, we simultaneously offer suggestions for future research. First, we collected data only in Indonesia. Thus, the generability of this study is limited to Indonesia. Different cultures, policies or work conditions might cause different effect on each of the constructs. Moreover, cultural dimensions might influence social norm (Hofstede and McCrae 2004). A person's intention to perform a behavior is influenced by the degree to which influential people support or admonish the outcome of a behavior (Ajzen 1991; Fishbein and Ajzen 1975). Future research can extend this study to other cultures or perform cross-cultural research to compare different effect of each construct in different cultural context. Second, our survey was limited to only three specific BYOD policy scenarios. Our study also omitted the intrusiveness of the BYOD ISSP to employees' privacy. The scenarios were regarded as the most common scenarios of BYOD security implementation in Indonesia based on out preliminary survey results. However, not all companies that implement BYOD have associated security policy in place. Thus, the number of input to determine the scenarios was limited. Furthermore, a variation of the intrusive level of a BYOD ISSP might create different employees' perception about the security policy. For example, it may result in different perceived levels of freedom threat and influence the compliance intention as a result of

employees' psychological reactance (Brehm 1966). Future research can consider more diverse scenarios and the intrusiveness of a BYOD ISSP.

9 Conclusions

The BYOD trend is inevitable in organizations. Yet, it raises serious concerns about information security. To the best of our knowledge, this study is the first empirical study to examine employees' compliance with organizational BYOD ISSP. Using reactance, perceived justice and protection motivation theories as a backdrop, this study shed light on the factors that influence employees' intention to comply with their organization's BYOD ISSP. An employee's perceived response efficacy and perceived justice would promote his intention to comply with the security policy. Restrictions imposed by an organization's BYOD ISSP could create a perception of freedom threat that could reduce an employee's intention to comply with BYOD ISSP. An employee's assessment of the costs associated with compliance behavior was found to intensify an employee's perception of freedom threat. We also demonstrated that BYOD security awareness programs might have both advantages and disadvantages. On the one hand, it could help to increase employees' perception of response efficacy. On the other hand, it could also increase employees' perception of response cost. This study also suggests the importance of having IT support team for BYOD as it would promote an employee's response efficacy and perceived digital mutualism justice. This study provides useful insights to organizations in shaping their BYOD implementation strategy. We hope that the findings of this study would stimulate further research in the IS security field.

APPENDIX A: CONSTRUCTS AND MEASUREMENTS

Intention to Comply	
INT1	I intend to comply with the requirements of my organization's BYOD ISSP.
INT2	I intend to protect my personal device used for work according to the requirements of my organization's BYOD ISSP.
INT3	I intend to carry out my responsibilities prescribed in my organization's BYOD ISSP when I use my personal device for work.
INT4	I am likely to follow my organization's BYOD ISSP.
INT5	There is a possibility that I will comply with my organization's BYOD ISSP to protect my organizational computing resources.
INT6	There is a possibility that I will comply with my organization's BYOD ISSP to protect my own device.
INT7	I am certain that I will follow my organization's BYOD ISSP.
Perceived Threat Vulnerability	
PV2	I could be subjected to an information security threat, if I don't comply with my organization's BYOD ISSP.
PV3	A security problem to my organization's information could occur if I don't comply with my organization's BYOD ISSP.
PV4	A security problem to my personal data could occur if I don't comply with my organization's BYOD ISSP.
Perceived Threat Severity	
PS1	If I don't comply with my organization's BYOD ISSP, there would be serious information security problems to my organization.
PS2	If I don't comply with my organization's BYOD ISSP, there would be serious information security problems to myself.
PS3	If I don't comply with my organization's BYOD ISSP, serious security problems to my organization's information would result.
PS4	If I don't comply with my organization's BYOD ISSP, serious security problems to my personal data would result.
Perceived response cost	
RC1	Complying with BYOD ISSP interferes with my work.
RC2	Complying with BYOD ISSP interferes with the personal use on my device.
RC3	There are too many overheads associated with complying with BYOD security policies.
RC4	Complying with BYOD ISSP would require considerable investment of effort other than time.

RC5	Complying with BYOD ISSP would take considerable amount of my working time.
RC6	Complying with BYOD ISSP would take considerable amount of my personal time.
Perceived response efficacy	
RE1	Complying with BYOD ISSP reduces the security threat to my organization's information.
RE2	Complying with BYOD ISSP reduces the security threat to my personal data.
RE3	If I comply with BYOD ISSP, mobile security problems in my organization will be scarce.
RE4	If I comply with BYOD ISSP, my mobile device related security problems will be scarce.
RE5	Compliance with BYOD ISSP helps to reduce IS security problems in my organization.
RE6	Compliance with BYOD ISSP helps me reduce security problems with my own personal data.
Perceived Freedom Threat	
FT1	The BYOD ISSP threatens my freedom to choose what I can do with my personal device.
FT2	The organization tries to make decisions for me through the BYOD ISSP.
Perceived digital mutualism justice	
PJ1	The requirements I have to fulfill due to the BYOD ISSP are fair considering my contribution to the company in using my own device.
PJ2	Obeying BYOD ISSP is fair considering my organization's responsibility in supporting BYOD.
PJ3	The benefits I provide my company by using my own device for work related tasks are fair considering the rewards I receive from my company.
PJ4	My contribution in using my own device is fair considering my organization's contribution in supporting BYOD.
BYOD security awareness program	
SET1	My organization provides training to improve employees' awareness of information security issues regarding the use of personal devices for work related tasks.
SET2	In my organization, employees are briefed on the risk to the organization of not securing mobile devices with a proper password.
SET3	In my organization, employees are briefed on the risk to the organization of not installing recommended anti-virus software on their mobile devices.
SET4	In my organization, employees are briefed on the risk to the organization of installing banned applications on their mobile devices.
SET5	In my organization, employees are briefed on the personal risk of not securing devices with a proper password.
SET6	In my organization, employees are briefed on the personal risk of not installing recommended anti-virus software on their mobile devices.
SET7	In my organization, employees are briefed on the personal risk of installing banned applications on their mobile devices.
SET8	My organization explains to employees about the responsibilities in using personal devices for work related tasks.
Organizational support	
OS1	My organization has an IT team that provides support to employees who use their personal device for work related tasks.
OS2	An IT support team is available to assist employees with their personal devices when needed.
OS3	The IT support team helps employees in following the requirements of the BYOD ISSP.
OS4	The IT support team helps employees if they encounter security problems on their personal devices.
Self-efficacy	
SE1	I would feel comfortable following most of the BYOD security policies on my own.
SE2	If I wanted to, I could easily follow BYOD security policies on my own.
SE3	I would be able to follow most of the BYOD security policies even if there was no one around to help me.

References

Adams, J.S. 1965. "Inequity in Social Exchange," in: *Advances in Experimental Social Psychology,* L. Berkowitz (ed.). New York: Academic Press.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp 179-211.

Ariyanto, A., Hornsey, M.J., and Gallois, C. 2006. "Group−Directed Criticism in Indonesia: Role of Message Source and Audience," *Asian Journal of Social Psychology* (9:2), pp 96-102.

Bagozzi, R.P., and Yi, Y. 1988. "On the Evaluation of Structural Equation Models," *Journal of the academy of marketing science* (16:1), pp 74-94.
Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychologcal Review* (84:2), pp 191-215.
Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American psychologist* (37:2), pp 122-147.
Beautement, A., Sasse, M.A., and Wonham, M. 2009. "The Compliance Budget: Managing Security Behaviour in Organisations," *Proceedings of the 2008 workshop on New security paradigms*: ACM, pp. 47-58.
Bies, R.J., and Moag, J.F. 1986. "Interactional Justice: Communication Criteria of Fairness," in: *Research on Negotiations in Organizations,* R.J. Lewicki, B.H. Sheppard and M.H. Bazerma (eds.). Greenwich, CT: JAI Press, pp. 43-55.
Bies, R.J., and Shapiro, D.L. 1987. "Interactional Fairness Judgments: The Influence of Causal Accounts," *Social Justice Research* (1:2), pp 199-218.
Bochner, S., and Hesketh, B. 1994. "Power Distance, Individualism/Collectivism, and Job-Related Attitudes in a Culturally Diverse Work Group," *Journal of Cross-Cultural Psychology* (25:2), pp 233-257.
Boer, H., and Seydel, E.R. 1996. "Protection Motivation Theory," in: *Predicting Health Behavior: Research and Practice with Social Cognition Models,* M. Connor and P. Norman (eds.). Buckingham, PA: Open University Press, pp. 95-120.
Brehm, J.W. 1966. *A Theory of Psychological Reactance*. New York: Academic Press.
Brehm, S.S., and Brehm, J.W. 1981. *Psychological Reactance: A Theory of Freedom and Control*. Academic Press New York.
Brehm, S.S., and Weinraub, M. 1977. "Physical Barriers and Psychological Reactance: 2-Yr-Olds' Responses to Threats to Freedom," *Journal of personality and social psychology* (35:11), p 830.
Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Mis Quarterly* (34:3), Sep, pp 523-548.
Chin, W.W. 1998. "The Partial Least Squares Approach for Structural Equation Modeling," in: *Methodology for Business and Management. Modern Methods for Business Research* G.A. Marcoulides (ed.). Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers, pp. 295-336.
Cisco. 2012. " Byod: A Global Perspective. Harnessing Employee-Led Innovation."
Citrix. 2011. "It Organizations Embrace Bring-Your-Own Devices."
Colquitt, J.A., Conlon, D.E., Wesson, M.J., Porter, C.O., and Ng, K.Y. 2001. "Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research," *Journal of Applied Psychology* (86:3), p 425.
Compeau, D.R., and Higgins, C.A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *Mis Quarterly* (19:2), pp 189-211.
Cook, K.S., and Hegtvedt, K.A. 1983. "Distributive Justice, Equity, and Equality," *Annual Review of Sociology* (9), pp 217-241.
Cropanzano, R., and Ambrose, M.L. 2001. "Procedural and Distributive Justice Are More Similar Than You Think: A Monistic Perspective and Research Agenda," in: *Advances in Organizational Justice,* J. Greenberg and R. Cropanzano (eds.). Stanford, CA: Stanford University Press, pp. 119-151.
D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp 79-98.
D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of Is Security Countermeasures," *Journal of business ethics* (89:1), pp 59-71.
Dabholkar, P.A., Thorpe, D.I., and Rentz, J.O. 1995. "A Measure of Service Quality for Retail Stores: Scale Development and Validation," *Journal of the academy of marketing science* (24:1), pp 3-16.
Dansereau, F., Alutto, J.A., Yammarino, F.J., and Dumas, M. 1984. *Theory Testing in Organizational Behavior: The Varient Approach*. Prentice-Hall Englewood Cliffs, NJ.

Dernbecher, S., Beck, R., and Weber, S. 2013. "Switch to Your Own to Work with the Known: An Empirical Study on Consumerization of It," *AMCIS 2013 Proceedings*.
Dillard, J.P., and Shen, L. 2005. "On the Nature of Reactance and Its Role in Persuasive Health Communication," *Communication Monographs* (72:2), pp 144-168.
Durbin, S. 2011. "Consumer Devices in the Workplace: A Best-Practice Security Approach," in: *Mobile Computing: Securing Your Workforce,* T.C.I.f.I. BCS (ed.). United Kingdom: British Informatics Society Limited, pp. 4-5.
Edwards, J.R. 2001. "Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework," *Organizational Research Methods* (4:2), pp 144-192.
Fishbein, M. 1963. "An Investigation of the Relationship between Beliefs About an Object and the Attitude toward That Object," *Human Relations*).
Fishbein, M., and Ajzen, I. 1975. *Theories of Attitude*. Reading, MA: Addison-Wesley.
Fishbein, M.E. 1961. "A Theoretical and Empirical Investigation of the Inter-Relation between Beliefs About an Object and the Attitude toward That Object."
Fornell, C., and Larcker, D.F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of marketing research*), pp 39-50.
Greenberg, J. 1987. "A Taxonomy of Organizational Justice Theories," *Academy of Management review*), pp 9-22.
György, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the Shadows: It Governance Approaches to User-Driven Innovation," *ECIS 2012 Proceding*.
Herath, T., and Rao, H.R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp 154-165.
Herath, T., and Rao, H.R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp 106-125.
Hofstede, G. 1983. "The Cultural Relativity of Organizational Practices and Theories," *Journal of International Business Studies* (14:2), pp 75-89.
Hofstede, G., and McCrae, R.R. 2004. "Personality and Culture Revisited: Linking Traits and Dimensions of Culture," *Cross-cultural research* (38:1), pp 52-88.
Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the Us and South Korea," *Information & Management* (49:2), pp 99-110.
Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp 83-95.
Lebek, B., Degirmenci, K., and Breitner, M.H. 2013. "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use Byod Mobile Devices," *AMCIS 2013 Proceeding*.
Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems* (48:4), pp 635-645.
Liputan6. 2013. "10 Prediksi Ict Di Indonesia Tahun 2013."
Loose, M., Weeger, A., and Gewald, H. 2013. "Byod–the Next Big Thing in Recruiting? Examining the Determinants of Byod Service Adoption Behavior from the Perspective of Future Employees,").
MacKenzie, S.B., Podsakoff, P.M., and Jarvis, C.B. 2005. "The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions," *Journal of Applied Psychology* (90:4), p 710.
MacKenzie, S.B., Podsakoff, P.M., and Podsakoff, N.P. 2011. "Construct Measurement and Validation Procedures in Mis and Behavioral Research: Integrating New and Existing Techniques," *Mis Quarterly* (35:2), pp 293-334.
Maddux, J.E., Norton, L.W., and Stoltenberg, C.D. 1986. "Self-Efficacy Expectancy, Outcome Expectancy, and Outcome Value: Relative Effects on Behavioral Intentions," *Journal of personality and social psychology* (51:4), p 783.

Maddux, J.E., and Rogers, R.W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp 469-479.
Maddux, J.E., Sherer, M., and Rogers, R.W. 1982. "Self-Efficacy Expectancy and Outcome Expectancy: Their Relationship and Their Effects on Behavioral Intentions," *Cognitive Therapy and Research* (6:2), pp 207-211.
Mahesh, S., and Hooter, A. 2013. "Managing and Securing Business Networks in the Smartphone Era," *Management Faculty Publications*.
Miller, K.W., Voas, J., and Hurlburt, G.F. 2012. "Byod: Security and Privacy Considerations," *IT Professional* (14:5), pp 53-55.
Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health−Related Behavior: A Meta−Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp 106-143.
MITTechnologyReview. 2012. "Ibm Faces the Perils of "Bring Your Own Device"." from http://www.technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device/
Murphy-Berman, V., and Berman, J.J. 2002. "Cross-Cultural Differences in Perceptions of Distributive Justice a Comparison of Hong Kong and Indonesia," *Journal of Cross-Cultural Psychology* (33:2), pp 157-170.
Niehaves, B., Köffer, S., and Ortbach, K. 2013. "The Effect of Private It Use on Work Performance-Towards an It Consumerization Theory," *Wirtschaftsinformatik*, p. 3.
Niehaves, B., Köffer, S., Ortbach, K., and Katschewitz, S. 2012. "Towards an It Consumerization Theory–a Theory and Practice Review," Westfälsche Wilhelms-Universität Münster (WWU)-European Research Center for Information Systems (ERCIS).
Ortbach, K., Bode, M., and Niehaves, B. 2013. "What Influences Technological Individualization?–an Analysis of Antecedents to It Consumerization Behavior," *AMCIS 2013 Proceedings*
Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pp. 156b-156b.
Peltier, T.R. 2005. "Implementing an Information Security Awareness Program," *EDPACS* (33:1), pp 1-18.
Pligt, J.v.d., and De Vries, N.K. 1998. "Expectancy-Value Models of Health Behaviour: The Role of Salience and Anticipated Affect," *Psychology and Health* (13:2), pp 289-305.
PricewaterhouseCoopers. 2012. "Bring Your Own Device: Agility through Consistent Delivery."
Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91:1), pp 93-114.
Schalow, P.R., Winkler, T.J., Repschlaeger, J., and Zarnekow, R. 2013. "The Blurring Boundaries of Work-Related and Personal Media Use: A Grounded Theory Study on the Employee's Perspective," *ECIS 2013 Proceedings*.
Setiadi, F., Sucahyo, Y.G., and Hasibuan, Z.A. 2012. "An Overview of the Development Indonesia National Cyber Security," *International Journal of Information Technology & Computer Science* (6).
Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in: *New Approaches for Security, Privacy and Trust in Complex Environments*. Springer, pp. 133-144.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *Mis Quarterly* (34:3), p 487.
Snyder, M.L., and Wicklund, R.A. 1976. "Prior Exercise of Freedom and Reactance," *Journal of Experimental Social Psychology* (12:2), pp 120-130.
Stagliano, T., DiPoalo, A., and Coonnelly, P. 2013. "The Consumerization of Information Technology," *Graduate Annual* (1:1), p 10.
Thibaut, J.W., and Walker, L. 1975. *Procedural Justice: A Psychological Analysis*. Hillsdale, N.J. and New York: L. Erlbaum Associates Hillsdale.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*).
Walker-Osborn, C., Mann, S., and Mann, V. 2013. "To Byod or … Not to Byod," *ITNOW* (55:1), March 1, 2013, pp 38-39.
Walster, E., Berscheid, E., and Walster, G.W. 1973. "New Directions in Equity Research," *Journal of personality and social psychology* (25:2), p 151.
Wetzels, M., Odekerken-Schroder, G., and Van Oppen, C. 2009. "Using Pls Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *Mis Quarterly* (33:1), pp 177-195.
Whitman, M.E. 2004. "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management* (24:1), pp 43-57.
Whitman, M.E., and Mattord, H.J. 2008. *Management of Information Security*, (2nd ed.). Course Technology Ptr.
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *Mis Quarterly* (37:1), pp 1-20.
Winquist, J.R., and Larson, J.R., Jr. 1998. "Information Pooling: When It Impacts Group Decision Making," *Journal of personality and social psychology* (74:2), pp 371-377.
Worchel, S., and Brehm, J.W. 1971. "Direct and Implied Social Restoration of Freedom," *Journal of personality and social psychology* (18:3), p 294.