ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 52, No.4: 657-674, December 2024
https://dx.doi.org/10.7469/JKSQM.2024.52.4.657

종업원의 BYOD 보안 정책 준수 의도에 영향을 미치는 사회 인지적 요인에 관한 연구

이창근* · 유준우* · 박준성* · 조영주* · 유준영* · 김소영* · 박희준*†

* 연세대학교 산업공학과

A Study on the Effect of Social Cognitive Factors on Employees' Intention to Comply with BYOD Security Policy

Lee, Chang Geun* · Yoo, Joon Woo* · Park, Jun Sung* · Cho, Young Ju* · Yoo, Jun Young* · Kim, So young* · Park, Hee Jun*†

* Department of Industrial Engineering, Yonsei University

ABSTRACT

Purpose: This study focuses on examining the social cognitive factors that influence employees' intentions to comply with security policies in a Bring Your Own Device (BYOD) environment, based on a model derived from Social Cognitive Theory. Additionally, it aims to propose managerial strategies to improve employees' adherence to BYOD security policies.

Methods: To investigate employees' intentions to comply with BYOD security policies, we performed hypotheses testing within the proposed research model. A Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis was employed to examine the collected data. The data was gathered from 268 employees working at companies that have adopted BYOD, through an online survey conducted between June 10 and 17, 2024.

Results: The results confirmed all of our proposed hypotheses. Encouragement by others, the information security practices by others and instrumental support significantly influence both outcome expectations and self-efficacy. Additionally, instrumental support, outcome expectations, and self-efficacy are shown to affect employees' intentions to comply with BYOD security policies.

Conclusion: Our study revealed that companies implementing BYOD should actively encourage employees to minimize security policy breaches by utilizing various support programs and sharing success stories of high performance resulting from adherence to the policies. This approach can effectively increase employees' intention to comply with BYOD information security policies.

Key Words: BYOD, Employees' Behavior, Security Policy Compliance Intention, Social Cognitive Theory, Technology Threat Avoidance Theory

● Received 7 October 2024, 1st revised 28 October 2024, accepted 5 November 2024
† Corresponding Author(h.park@yonsei.ac.kr)

* 본 연구는 연세대학교 이창근 석사학위 논문의 일부를 재구성한 내용임

1. Introduction

Smart work environment has been brought through the popularization of developed electronic devices such as smart phones or tablets and the high-speed internet (Abiodun et al., 2023). Various organizations endeavor to adopt remote work, shared offices, etc (Lee & Seol, 2021). In particular, BYOD practice was inevitable in workplaces since maintaining the operations by connecting with employees remotely in social distancing situations has been emphasized during the COVID-19 pandemic (Lee et al., 2022; Seo et al., 2022). As time passes, an influx of young and new workers who have grown up with developed technologies and demand to use what they utilize in their daily lives also tend to increase progressively (Jarrahi et al., 2017).

As the trend continues, BYOD was introduced as a revolutionary work system which encourages employees to shift away from the traditional use of shared devices, with the goal of streamlining work processes and fostering corporate innovation. This system involves individuals bringing and using personal smart devices at work or in learning environments (Palanisamy et al., 2022; Singh, 2012). With the growth of smart work practices, the BYOD industry gained significant traction, estimating a $367 billion market size by 2022 compared to $30 billion in 2014 (Bullock, 2019).

The advantages of BYOD can be listed as follows. On the individual level, the use of personal devices enables employees to overcome time limitations and manage their schedules more flexibly. Employees can reduce spatial and temporal constraints by engaging in practices like remote work and flexible seating arrangements (Eslahi et al., 2014). On the organizational side, BYOD allows companies to save on the costs and time involved in purchasing and managing devices, ultimately contributing to the goal of improving productivity (Eslahi et al., 2014).

However, BYOD also presents security risks, such as data breaches, since personal devices have direct access to corporate networks. The loss or theft of these devices can lead to the exposure of sensitive company data and personal information, which could negatively impact organizational efficiency (Lee Jr et al., 2017). To mitigate such risks, previous BYOD studies have primarily focused on enhancing security technologies to support the secure implementation of BYOD while minimizing corporate security threats (Cho & Ip, 2018). However, prior research has increasingly indicated that most security issues stem from employee behavior. For instance, Pahnila et al. (2007) highlighted the need to consider non-technical factors, such as employee motivation, alongside technical solutions, emphasizing the role of employee attitudes toward compliance with security policies. Moreover, Timms (2017) observed that while many organizations implement security policies to counter BYOD-related threats, employees often disregard these measures, with many security breaches traced back to negligent employee behavior. Consequently, several studies have argued that addressing BYOD security vulnerabilities should focus more on human factors than solely on technological advancements.

To ensure security while expanding BYOD use within companies, it is essential to raise awareness and encourage adherence to security policies among employees (Caballero, 2017). There remains a necessity to understand what drives employees to follow BYOD security policies utilizing conceptual theory reflecting social factors, since past studies have primarily used TTAT (Technology Threat Avoidance Theory) and PMT (Protection Motivation Theory) as conceptual research model to explain employee behavior without taking environmental factors into account (Crossler et al., 2014; Yim, 2021; Siponen et al., 2006). In addition, there is little quantitative research analyzing the direct impact of organizational support on employees' BYOD security policy compliance intention. Therefore, it is necessary to study employees' security policy compliance intention considering the surrounding environment since BYOD is a system which is utilized within working environments and all employees are required to follow the policies established by the organization.

This study seeks to examine the factors that influence employees' intention to comply with BYOD security policies in companies that have adopted BYOD. The analysis will be based on Social Cognitive Theory from the organizational perspective and propose managerial strategies to improve employees' security policy compliance. The findings of this study could inform the development of information security strategies that promote policy compliance among employees in organizations that have already adopted or are planning to adopt BYOD.

2. Conceptual background and Literature Review

2.1 BYOD Security Policy Compliance Research

As organizations transition towards fostering a smart work culture, many companies have adopted BYOD as a strategic approach. This change has sparked a wide range of research on BYOD from multiple viewpoints. Specifically, some studies have focused on exploring user behavioral intentions concerning adherence to BYOD security policies. These studies span various education or work settings, including corporate businesses and public institutions.

For example, Crossler et al. (2014) investigated the factors that shape students' and employees' intentions to comply with BYOD policies using PMT. They found that self-efficacy and response efficacy were key determinants of users' intentions to adhere to security guidelines. Putri and Hovav (2014) analyzed employees' intention to comply with BYOD security policy with a research model incorporating reactance, protection motivation and organizational justice theories. They argued that perceived response efficacy and justice have a positive impact on employees' intention, perceived freedom threat negatively affects employees' intentions to comply with security policy, and suggested the importance of organizational support team. In the public sector, Palanisamy et al. (2024) examined the influence of perceived mandatoriness, self-efficacy, and psychological ownership on employees' compliance intentions in public institutions, employing a model that integrated OCT, Security Culture, and SCT.

Although research on user behavior regarding BYOD security compliance has been extensive, there are very few studies that have analyzed employees' BYOD security policy compliance intentions from social factors. Since BYOD is a practice used in organizations, it is necessary to consider that the BYOD security policy compliance behavior of employees is influenced by their surroundings. Thus it can play a critical role to improve employees' security practices.

2.2 Social Cognitive Theory (SCT)

To highlight how human behavior and cognitive processes are shaped by the interplay between personal attributes, the environment, and actions, Bandura (1986) proposed Social Cognitive Theory (SCT). SCT suggests that learning takes place through actions and thoughts, which are influenced by environmental and situational factors, emphasizing the critical role of motivation and expected performance in encouraging positive behavior. Consequently, SCT has become a foundational theory in various fields studying behavioral factors within organizations.

For example, Borah et al. (2024) examined the factors influencing recommended COVID-19 health behaviors within the framework of SCT. They argued that self-efficacy played a major role in shaping these health behaviors, while outcome expectancies also significantly influenced adherence to COVID-19 guidelines. Similarly, Al-Dokhny et al. (2021) conducted an empirical study on students' intentions to use remote education platforms by integrating the Technology Acceptance Model (TAM) with SCT. Their findings demonstrated that self-efficacy had a strong influence on perceived usefulness and practicality, both of which affected the students' intentions to use the platforms. Furthermore, Boateng et al. (2016) explored the factors that affect users' internet banking adoption intention by applying a research model grounded in SCT. They found that social features of websites which enable customers to communicate with other user, trust from using internet banking platform, compatibility with lifestyle significantly impacts customers' intentions for internet banking adoption.

Regarding Social Cognitive Theory that the social environment plays a crucial role in shaping individual behavior, there is an increasing demand for research with SCT analyzing employees' behavior considering the surrounding environment. Therefore, this study seeks to analyze the factors that influence employees' intentions to comply with BYOD security policies by Social Cognitive Theory which explores behavior as influenced by the surrounding environment, and empirically identify the direct effect between instrumental support and security policy compliance intention.

3. Methodology

3.1 Research Model

This study aims to identify the social cognitive factors influencing employees' intentions to comply with

BYOD security policies based on SCT. Accordingly, we constructed the following research model which is developed from SCT grounded in relevant past studies Figure 1.

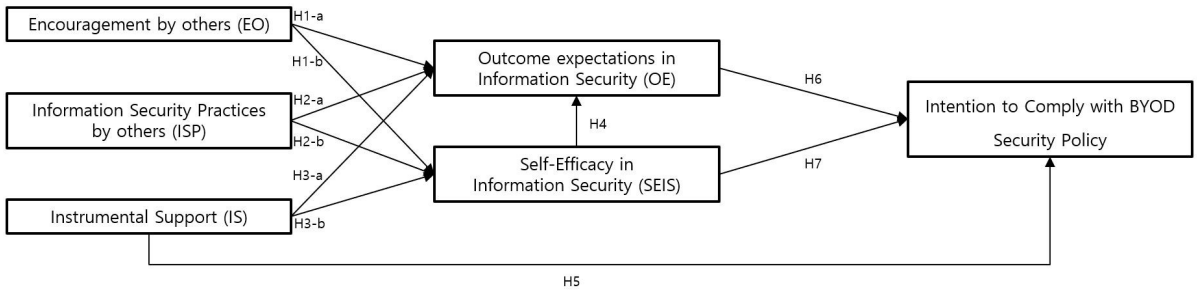

Figure 1. Proposed Research Model

3.2 Research Hypothesis

As outlined by Social Cognitive Theory (SCT), individuals engage in reciprocal interactions with others to acquire new knowledge and behaviors by observing their environment. Specifically, people who are influenced by external factors such as social pressure or encouragement by others which can be defined as the degree of persuasion from other employees to comply with BYOD security policies tend to perceive these influences and adjust their behavior accordingly through self-efficacy and performance expectations (Compeau & Higgins, 1995). Furthermore, Keyvani & Mozafari (2009) suggested that encouragement enhances an individual's ability to boost self-esteem and resilience. Similarly, Hsu et al. (2021) found that students' awareness of faculty encouragement positively influences their self-efficacy. Based on the prior studies, we hypothesize that the encouragement from colleagues and superiors to adhere to BYOD security policies will positively affect employees' outcome expectations and self-efficacy regarding compliance with these policies.

H1-a: The encouragement by others to comply with BYOD security policies positively impacts outcome expectations in information security.

H1-b: The encouragement by others to comply with BYOD security policies positively impacts self-efficacy in information security.

Instrumental support, such as security training programs and the involvement of experts, can be defined as the extent of organizational assistance to encourage BYOD security policies compliance (Galvez et al., 2015). It is expected to help individuals recognize the benefits of their environment and achieve positive outcomes through their actions. Compeau and Higgins (1995) argued that computer users experience improvements in their abilities and self-efficacy when they perceive organizational support, such as assistance from security experts. Additionally, Galvez et al. (2015) noted that systematic support for employees reduces the risk of safety incidents within organizations. Therefore, organizational efforts to enhance com-

pliance with BYOD security policies, through support initiatives, are likely to have a positive impact on employees' outcome expectations and self-efficacy in organizations that have adopted BYOD.

H2-a: Instrumental support to comply with BYOD security policies positively impacts outcome expectations in information security.

H2-b: Instrumental support to comply with BYOD security policies positively impacts self-efficacy in information security.

Individuals learn new information and select behaviors by observing others (Bandura, 1986). For example, Galvez et al. (2015) argued that within management information systems, observing the security practices of others increases individual self-efficacy and performance expectations, which in turn encourages them to engage in these practices themselves. Similarly, Kwon et al. (2022) found that in sports competitions, observational learning enhances athletes' self-efficacy their performance. Based on prior research, it is evident that information security practices by others which can be defined as observational learning from other employees complying with BYOD security policies impacts self-efficacy and performance expectations. Therefore, we hypothesize that observing others' information security practices will positively affect employees' performance expectations and self-efficacy in complying with BYOD security policies.

H3-a: Information security practices by others positively impacts outcome expectations in information security.

H3-b: Information security practices by others positively impacts self-efficacy in information security.

Self-efficacy refers to an individual's belief in their ability to successfully carry out a specific task (Ajzen, 2005). Higher levels of self-efficacy motivate individuals to participate more actively in tasks, thereby leading to enhanced performance expectations (Galvez et al., 2015). For instance, Domenech et al. (2017) demonstrated that students with greater self-efficacy have higher expectations for academic success. Similarly, in this study, it is anticipated that employees who possess high self-efficacy regarding BYOD security practices will achieve superior work performance.

H4: Self-efficacy in information security positively impacts outcome expectations in information security.

Organizational support is a kind of managerial solutions to spurring employees' behavioral improvement. Organizations can implement instrumental aid programs, such as SETA (Security Education, Training, Awareness). It targets users in an organization to help them to be aware of appropriate information security practices. Then, employees make efforts to develop their security skills understand how to perform their work securely (Caballero, 2017). In accordance with employees' endeavor, they will be more conscious of security behavior (Ng et al., 2009). Therefore, we hypothesize that instrumental support will positively influence employees' BYOD security policies compliance intention.

H5: Instrumental Support positively impacts the intention to comply with BYOD security policy.

Performance expectations serve as crucial predictors of whether individuals will carry out specific behaviors (Galvez et al., 2015). When people believe that their desired outcomes are attainable, they are more motivated to engage in those behaviors (Lin & Chang, 2018). As performance expectations increase, so does the intention to act, as heightened motivation often drives the behavior (Chao, 2019). Based on this, it is anticipated in this study that employees with higher performance expectations are more likely to lead to compliance with BYOD security policies.

H6: Outcome expectations in information security positively impacts the intention to comply with BYOD security policy.

As users build self-efficacy through various experiences and by overcoming obstacles, their motivation to believe in their capabilities and act increases (Liu et al., 2022). Specifically, users with high self-efficacy in security-related activities are more inclined to adopt security innovations and take proactive measures (Hameed & Arachchilage, 2021). Conversely, lower motivation often results in self-doubt and a reluctance to engage in certain behavior (Pákozdy et al., 2024). Thus, we hypothesize that self-efficacy related to following BYOD security policies will positively influence users' intentions to comply with these policies.

H7: Self-efficacy in information security positively impacts the intention to comply with BYOD security policy.

4. Results

4.1 Data Collection

To select and ensure an appropriate sample, it is necessary to confirm whether respondents are working at a company that has adopted BYOD and to minimize survey limitations, such as respondent bias. So, we specified the definition of BYOD in the questionnaire and participants were asked to answer a screening question, “Do you use your own devices for work in your work environment?” before participating in the survey. All responses were measured on a 5-point Likert scale, and survey items were developed items were developed from prior SCT studies. A pilot test was conducted with 50 participants to refine the survey process and clarify vague measurement items. Afterward, we developed the final questionnaire as shown in Table 1.

Table 1. Survey Items

Variable	Item	Measure	Ref.
Encouragement by Others (EO)	EO1	I was encouraged to use my own devices by peers in my work organization	Compeau & Higgins (1995)
	EO2	I was encouraged to use my own devices by peers in other work organizations	
	EO3	I was encouraged to use my own devices by subordinates in my work organization	
Instrumental Support (IS)	IS1	I was encouraged by my work organization offering training activities to comply information security policy	Alvarez et al. (2022)
	IS2	I was encouraged by my work organization offering information security software for each type of device	
	IS3	Someone would help me when I need help to comply information security policy	
Information Security Practices by others (ISP)	ISP1	I was encouraged by peers in my work organization practicing information security	Compeau & Higgins (1995); Compeau & Higgins (1999)
	ISP2	I was encouraged by peers in other work organization practicing information security	
	ISP3	I was encouraged by managers in my work organization practicing information security	
	ISP4	I was encouraged by subordinates in my work organizations practicing information security	
Outcome Expectations in Information Security (OE)	OE1	If I comply with the information security policy, I will increase my sense of accomplishment	
	OE2	If I comply with the information security policy, I will increase my chances of obtaining a promotion	
	OE3	If I comply with the information security policy, I will be seen as higher in status by my peers	
Self-Efficacy in Information Security (SE)	SE1	Complying with information security policy is a task I can perform	Alvarez et al. (2022); Kwon & Lee (2022)
	SE2	I have sufficient technological skills to comply information security policy	
	SE3	I will be able to complete my task with my own device if I have information security manuals	
Intention to Comply with BYOD Security Policy (ICSP)	ICSP1	I intend to comply with the requirements of the BYOD information security policy of my organization	Herath & Rao (2009)
	ICSP2	I will follow the BYOD information security policy of my organization in the future	

After refining the survey, 282 responses were collected from June 10 to June 17, 2024, using Amazon mTurk. After eliminating 14 insincere responses, 268 responses were analyzed in this study. Detailed demographic characteristics of the respondents are presented in Table 2.

Table 2. Demographics of Respondents

Classification		Frequency (N=268)	Percentage (%)
Gender	Male	193	72.01%
	Female	75	27.99%
Age	20 to 29	91	33.96%
	30 to 39	143	53.36%
	40 to 49	20	7.46%
	Above 50	14	5.22%
Education Level	Elementary/Middle School	6	2.24%
	High School	20	7.46%
	University/College Degree	228	85.07%
	Graduate School	14	5.22%
Work Experience	Less than 1 year	6	2.24%
	1-5 years	95	35.45%
	6-10 years	125	46.64%
	11-15 years	39	14.55%
	16 years above	3	1.12%

4.2 Research Method

The research model in this study was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). PLS-SEM offers distinct advantages in analyzing complex research models by measuring relationships and explanatory power between variables through both measurement and path analysis (Hair et al., 2017). It is particularly beneficial for estimating parameters efficiently and evaluating structural models when working with relatively small sample sizes, as it provides higher statistical power compared to Covariance-Based SEM (CB-SEM) (Hair et al., 2019). For these reasons, this study employed SmartPLS 4.0 software to conduct the PLS-SEM-based analysis, ensuring efficient validation of the complex research model, which includes various variables and a limited sample size.

4.3 Results of Analysis

We validated the proposed structural model and hypotheses in this study by thoroughly analyzing the reliability and validity of the measurement items. For reflective measurement models, the factor loading values must exceed 0.7 to confirm the reliability of each item. Additionally, Composite Reliability (CR) and Cronbach's alpha values should be greater than 0.7 to establish internal consistency reliability. Convergent validity is then assessed by examining the average variance extracted (AVE) values, where the AVE for each construct must surpass 0.5 (Fornell & Larcker, 1981).

As presented in Table 3, the results of the reliability analysis, internal consistency reliability, and convergent validity for each measurement item in this study meet all of the specified evaluation criteria, con-

firming the robustness of the measurement model.

Table 3. Results of the Validity test

Variable	Factor loadings	AVE	CR	Cronbach's alpha
EO	0.731 0.866 0.855	0.672	0.859	0.754
IS	0.814 0.783 0.845	0.663	0.855	0.747
ISP	0.750 0.720 0.747 0.773	0.559	0.835	0.738
OE	0.801 0.740 0.861	0.644	0.844	0.721
SE	0.837 0.818 0.772	0.655	0.850	0.736
ICSP	0.874 0.884	0.773	0.872	0.706

Discriminant validity refers to the extent to which latent variables are distinct from one another. In this study, the Fornell-Larcker criterion was employed. In Table 4, the diagonal values represent the square root of the AVE, which must exceed the highest correlation between the latent variables to demonstrate discriminant validity (Fornell & Larcker, 1981). As indicated in Table 4, the discriminant validity results meet the required criteria.

Table 4. Results of Discriminant Validity test (Fornell-Larcker criterion)

	EO	IS	ISP	OE	SE	ICSP
EO	**0.820**					
IS	0.752	**0.814**				
ISP	0.734	0.742	**0.748**			
OE	0.717	0.733	0.729	**0.802**		
SE	0.684	0.735	0.659	0.753	**0.809**	
ICSP	0.603	0.676	0.584	0.668	0.680	**0.879**

As confirmed in Table 3 and Table 4, the reliability and validity of the research model have been successfully established, allowing us to proceed with testing the research hypotheses through an evaluation of the structural model. The structural model evaluation will consider multicollinearity (VIF), the coefficient of determination (R^2), effect size, and the significance and relevance of the path coefficients. First, multicollinearity is assessed by examining the inner VIF values among latent variables, with values below 5 indicating no multicollinearity issues (Hair et al., 2017). As shown in Table 5, none of the variables exhibit multicollinearity.

Next, the coefficient of determination (R^2) measures the explanatory power of the structural model, ranging from 0 to 1, with values closer to 1 indicating greater predictive accuracy. Generally, an R^2 of 0.25 is considered weak, 0.5 is moderate, and 0.75 or higher is considered strong (Hair et al., 2017). In this study, the adjusted R^2 values for OE, SE, and ICSP were 0.684, 0.585, and 0.546, respectively, all exceeding 0.5, which indicates a moderate explanatory power.

Table 5. Results of Collinearity test (VIF)

	OE	SE	ICSP
EO	2.876	2.738	
IS	3.279	2.810	2.599
ISP	2.707	2.646	
OE			2.755
SE	2.438		2.774

The results of the path analysis are presented below in Table 6. The hypotheses were tested using a bootstrapping procedure.

EO was found to have a positive effect on OE ($\beta = 0.171$, $p = 0.011$) and SE ($\beta = 0.238$, $p = 0.003$), thus supporting both H1-a and H1-b. IS also showed a positive impact on OE ($\beta = 0.155$, $p = 0.029$) and SE ($\beta = 0.439$, $p = 0.000$), which accept H2-a and H2-b. ISP positively affected OE ($\beta = 0.255$, $p = 0.000$) and SE ($\beta = 0.159$, $p = 0.047$), thus supporting H3-a and H3-b. Also, SE was found to have a substantial effect on OE ($\beta = 0.354$, $p = 0.000$), thereby validating H4.

In addition, IS, OE and SE were found to directly influence the ICSP ($\beta = 0.290$, $p = 0.000$; $\beta = 0.241$, $p = 0.002$; $\beta = 0.286$, $p = 0.000$), leading to the acceptance of H5, H6 and H7. Regarding overall results, among the factors that directly influence BYOD security policy compliance, IS showed higher impact than other variables.

Moreover, from the classification by Cohen (2013), the effect size(f^2) is considered weak if it is greater than 0.02 and moderate if it exceeds 0.15.

Table 6. Result of Path Analysis

Path	Hypothesis	Beta	t value	p-value	Result	f^2
EO → OE	H1-a	0.171	2.540	0.011	Supported	0.032
EO → SE	H1-b	0.238	2.998	0.003	Supported	0.050
IS → OE	H2-a	0.155	2.186	0.029	Supported	0.024
IS → SE	H2-b	0.439	5.136	0	Supported	0.167
ISP → OE	H3-a	0.255	3.988	0	Supported	0.077
ISP → SE	H3-b	0.159	1.990	0.047	Supported	0.023
SE → OE	H4	0.354	3.920	0	Supported	0.165
IS → ICSP	H5	0.290	3.725	0	Supported	0.072
OE → ICSP	H6	0.241	3.102	0.002	Supported	0.047
SE → ICSP	H7	0.286	4.177	0	Supported	0.066

5. Conclusion

This study aimed to explore the social cognitive factors influencing employees' BYOD security policy compliance. The findings revealed that EO, IS and ISP significantly influence OE and SE in relation to BYOD security policy compliance. These results align with existing studies which emphasize the impacts of social cognitive factors on performance expectation and self-efficacy (Compeau & Higgins, 1995; Galvez & Guzman, 2009; Galvez et al., 2015).

Also, it was observed that SE has a positive effect on OE. This finding is consistent with the study of Galvez et al. (2015), which indicated that higher levels of self-efficacy lead to higher performance expectations. Additionally, IS, OE and SE were found to influence employees' BYOD security policy compliance intention. This aligns with previous research showing that organizational efforts such as security education and security training show a positive influence on employees' behavior improvement (Ng et al., 2009), individuals' outcome expectations regarding information security positively affect compliance with security rules (Galvez et al., 2015), and self-efficacy concerning security policy compliance positively influences employees' intent to follow BYOD security policies (Ifinedo, 2014; Siponen et al., 2014). Therefore, all hypotheses are verified and supported through empirical approach.

5.1 Theoretical Implication

Our study identified the factors that influence employees' intention to comply with BYOD security policies from an organizational perspective, emphasizing the impact of the surrounding environment. However, there is a scarcity of studies utilizing Social Cognitive Theory, which takes into account encouragement, support from others, and observational learning. Previous research in this field includes Crossler et al. (2014), who analyzed employees' BYOD policy compliance behavior through the lens of PMT, and Hovav and Putri (2016), who combined PMT, Reactance Theory, and Organizational Justice Theory (OJT) to study

effective technical approaches for addressing BYOD security policy compliance. Given that BYOD is increasingly adopted within organizations alongside advancements in information security technologies, this study applied Social Cognitive Theory, which considers the influence of organizational environments on individual behavior. We believe the research model proposed in this study offers a valuable framework for analyzing user security behavior.

Secondly, to the best of our knowledge, this is the first study to directly examine the relationship between instrumental support and employees' intention to comply with BYOD security policies, while also suggesting managerial strategies for establishing effective support programs. Previous studies primarily showed that organizational support influences outcome expectations or self-efficacy, which in turn affects compliance intention (Hovav & Putri, 2016; Palanisamy et al., 2024). However, since this study empirically verified the direct influence of instrumental support on BYOD security policy compliance intentions, it can serve as a foundation for future analyses of security behavior. Moreover, it provides insights for developing organizational strategies, such as security education, training programs, and awareness initiatives that highlight the importance of organizational support.

5.2 Practical Implication

The BYOD market continues to grow due to advancements in information security technologies and shifts in work and educational environments with employees' needs. On account of increasing interest for BYOD from the adoption of the revolutionary work environment such as hot-desking, the BYOD industry is expected to expand to a market size of $430 billion dollars by 2025 (Velzian, 2021). However, while these innovative work settings and technologies offer flexibility, they also pose significant risks to a company's information security systems. Therefore, it is crucial for organizations to take proactive measures to address these challenges (Ponemon, 2016). To ensure the sustainable implementation and operation of BYOD, companies should consider the following managerial strategies to encourage employees to develop more positive attitudes toward information security policies.

According to the findings of our study, instrumental support emerged as the most influential social factor affecting compliance intention. Based on these results, we emphasize the importance of robust organizational efforts to foster and reinforce BYOD security policy compliance intentions. Previous research has also indicated that organizational support is a key strategy for improving the practicality of security policy compliance (Hwang et al., 2017). Companies should take into account employees' personal relevance and level of knowledge to maximize the effectiveness of support activities when designing appropriate policy compliance training programs (Alshaikh et al., 2020; Puhakainen & Siponen, 2010). Therefore, to promote BYOD security policy compliance, companies should offer differentiated support activities tailored to various employee groups, based on job position, experience, and other factors. In conclusion, organizations need to implement more dynamic and customized support initiatives, as tailored instrumental support can greatly enhance employees' self-efficacy and, consequently their intentions to comply with BYOD security policies.

Secondly, considering the study by Seneviratne & Hewakuruppuge (2023), user-generated content like case studies promotes a culture of shared expertise and knowledge among employees. Applying these findings to our research, organizations can motivate compliance by sharing success stories or failure precedents related to BYOD policy adherence or non-compliance. When employees can foresee the potential outcomes of their actions, they are more likely to follow the rules (Tai, 2006). Therefore, companies should cultivate a corporate education culture that raises awareness of the importance of security policy compliance, taking into account the varying backgrounds of employees. These insights can be pivotal in shaping organizational support strategies that enhance BYOD security policy compliance across the organization.

In light of the above, organizations can offer tailored security support programs that take into account employees' roles, departments, and specific security challenges they might encounter. Such a program could include sharing actual cases of security breaches relevant to each position or department. For instance, employees in sales roles, who frequently exchange data with external parties, could benefit from training focused on data leakage prevention and secure communication practices. Meanwhile, those in R&D might receive targeted guidance on safeguarding intellectual property. This approach promotes engagement and mutual understanding among employees, enhancing compliance by encouraging feedback on security practices. By collecting and integrating this interaction, organizations can continuously refine security policies, thereby fostering a culture of proactive security awareness and policy adherence.

5.3 Limitations and Future Research Recommendations

While this study offers valuable theoretical and managerial implications by identifying the factors influencing employees' policy compliance intentions, there are some limitations that must be addressed. We would like to suggest directions for future research to overcome these limitations.

First, although this study provides insights into the factors that influence employees' behavioral intentions, it does not investigate whether these intentions lead to actual compliance behavior. Future research should explore employees' real compliance behaviors to better understand the gap, if any, between intention and action. It could help in assessing the effectiveness of the strategies aimed at fostering compliance intentions and the scope of the research can be expanded to propose advanced managerial strategies based on the analysis of actual compliance behaviors.

Second, as BYOD has recently emerged alongside advancements in security technologies, certain users may avoid BYOD adoption due to perceived threats. To address this issue, it is essential to consider individual intentions to avoid technology. We propose that future research integrate TTAT to examine users' intentions to avoid technological threats, which can provide a more comprehensive understanding of resistance to BYOD adoption.

Despite these limitations, our study highlights the significant influence of social environments on employees' compliance behavior with BYOD security policies. It also emphasizes the importance of strategic organizational support in encouraging policy adherence. Given these contributions, our research can serve as a strong foundation for future studies in this area.

REFERENCES

Abiodun, T., Rampersad, G., & Brinkworth, R. Driving industrial digital transformation. Journal of Computer Information Systems. 2023, 63(6):1345-1361.

Ajzen, I. (2005). Attitudes, personality and behaviour. McGraw-hill education (UK).

Al-Dokhny, A., Drwish, A., Alyoussef, I., & Al-Abdullatif, A. 2021. Students' intentions to use distance education platforms: An investigation into expanding the technology acceptance model through social cognitive theory. Electronics 10(23):2992.

Alvarez-Risco, A., Del-Aguila-Arcentales, S., Rosen, M. A., & Yáñez, J. A. 2022. Social Cognitive Theory to Assess the Intention to participate in the Facebook Metaverse by citizens in Peru during the COVID-19 pandemic. Journal of Open Innovation: Technology, Market, and Complexity 8(3):142.

Bandura, A. 1986. Social foundations of thought and action. Englewood Cliffs 23-28, 2.

Boateng, H., Adam, D. R., Okoe, A. F., & Anning-Dorson, T. (2016). Assessing the determinants of internet banking adoption intentions: A social cognitive theory perspective. Computers in Human Behavior, 65, 468-478.

Borah, P., Lorenzano, K., Yel, E., & Austin, E. 2024. Social cognitive theory and willingness to perform recommended health behavior: the moderating role of misperceptions. Journal of Health Communication 29(1):49-60.

Bullock, L. (2019). The future of byod: Statistics, predictions and best practices to prep for the future. Forbes.

Caballero, A. (2017). Security education, training, and awareness. In Computer and information security handbook (pp. 497-505). Morgan Kaufmann.

Chao, C. M. 2019. Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. Frontiers in psychology 10:1652.

Cho, V., Ip, W. H. 2018. A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. Enterprise Information Systems 12(6):659-673.

Cohen, J. 2013. Statistical power analysis for the behavioral sciences. routledge.

Compeau, D. R., & Higgins, C. A. 1995. Computer self-efficacy: Development of a measure and initial test. MIS quarterly 189-211.

Compeau, D., Higgins, C. A., & Huff, S. 1999. Social cognitive theory and individual reactions to computing technology: A longitudinal study. MIS quarterly 145-158.

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.

Doménech-Betoret, F., Abellán-Roselló, L., & Gómez-Artiga, A. 2017. Self-efficacy, satisfaction, and academic achievement: the mediator role of Students' expectancy-value beliefs. Frontiers in psychology, 8, 1193.

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., & Saad, E. H. M. (2014, April). BYOD: Current state and security challenges. In 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE) (pp. 189-192). IEEE.

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

Galvez, S. M., & Guzman, I. R. 2009. Identifying factors that influence corporate information security behavior. AMCIS 2009 Proceedings, 765.

Galvez, S. M., Shackman, J. D., Guzman, I. R., & Ho, S. M. 2015. Factors affecting individual information security practices. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, 135-144.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European business review, 31(1), 2-24.

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. 2017. An updated and expanded assessment of PLS-SEM in information systems research. Industrial management & data systems 117(3):442-458.

Hameed, M. A., & Arachchilage, N. A. G. 2021. The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment. Personal and Ubiquitous Computing 25(5):911-925.

Herath, T., & Rao, H. R. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems 18(2):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.

Hsu, H. Y., Li, Y., Dugger, S., & Jones, J. 2021. Exploring the relationship between student-perceived faculty encouragement, self-efficacy, and intent to persist in engineering programs. European Journal of Engineering Education 46(5):718-734.

Hwang, I., Kim, D., Kim, T., & Kim, S. 2017. Why not comply with information security? An empirical approach for the causes of non-compliance. Online Information Review 41(1):2-18.

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

Jarrahi, M. H., Crowston, K., Bondar, K., & Katzy, B. (2017). A pragmatic approach to managing enterprise IT infrastructures in the era of consumerization and individualization of IT. International Journal of Information Management, 37(6), 566-575.

Keyvani, A., & Mozafari, M. 2009. Encouragement, punishment, offering new solutions. International Journal of Management Perspectives 1(4):74-85.

Kwon, D, H & Lee, S, H. 2022. A Study on the Mediating Effect of Self-Efficacy in the Relationship between Self-leadership and Customer Orientation: Focusing on Airline Cabin Crew. Journal of Korean Society for Quality Management 50(3):441-457.

Kwon, T., Shin, S., & Shin, M. 2022. The effect of observational learning on self-efficacy by sport competition condition, performance level of team members, and whether you win or lose. International Journal of Environmental Research and Public Health 19(16):10148.

Lee Je Hyeon, Seol Hyun Do. 2021. A Study on Change Issues and Overcoming Measures in the Adoption of Smart Work - Focusing on Leadership, Communication, Organizational Culture, and Human Resource Management Aspects. The e-Business Studies 22(1):107-121.

Lee Jr, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. 2017. Implications of monitoring mechanisms on bring your own device adoption. Journal of Computer Information Systems 57(4):309-318.

Lee, S, An, J, and Yun, H 2022. Examining User Perception about Airline Untact Service Quality. Journal of Korean Society for Quality Management 50(3):545-570.

Lin, H. C., & Chang, C. M. (2018). What motivates health information exchange in social media? The roles of the social cognitive theory and perceived interactivity. Information & Management, 55(6), 771-780.

Liu, J., Zeng, M., Wang, D., Zhang, Y., Shang, B., & Ma, X. (2022). Applying social cognitive theory in predicting physical activity among Chinese adolescents: a cross-sectional study with multigroup structural equation model. Frontiers in psychology, 12, 695241.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Pahnila, S., Siponen, M., & Mahmood, A. 2007. Employees' behavior towards IS security policy compliance. In 2007 40th Annual Hawaii International Conference on System Sciences, 156b.

Pákozdy, C., Askew, J., Dyer, J., Gately, P., Martin, L., Mavor, K. I., & Brown, G. R. 2024. The imposter phenomenon and its relationship with self-efficacy, perfectionism and happiness in university students. Current Psychology 43(6):5153-5162.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. 2022. BYOD policy compliance: Risks and strategies in organizations. Journal of Computer Information Systems 62(1):61-72.

Palanisamy, R., Norman, A. A., Mat Kiah, M. L. 2024. Employees' BYOD security policy compliance in the public sector. Journal of Computer Information Systems 64(1):62-77.

Ponemon, I. 2016. Sixth annual benchmark study on privacy & security of healthcare data. Technical Report.

Puhakainen, P., & Siponen, M. 2010. Improving employees' compliance through information systems security training: an action research study. MIS quarterly, 757-778.

Seneviratne, P., & Hewakuruppuge, R. H. 2023. The Market Orientation and User Generated Content for Knowledge Sharing.

Seo Jay, An Sunju, Choi Jeongil. 2022. A Study on Factors Affecting Intention to Use Online Collaboration Tools for the Non-Face-to-Face Educational Environment. Journal of Korean Society for Quality Management. 50(3):571-591.

Singh, N. 2012. BYOD genie is out of the bottle"Devil or angel". Journal of Business Management & Social Sciences Research 1(3):1-12.

Siponen, M., Mahmood, M. A., & Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. Information & management 51(2):217-224.

Siponen, M., Pahnila, S., & Mahmood, A. (2006, November). Factors influencing protection motivation and IS security policy compliance. In 2006 Innovations in Information Technology (pp. 1-5). IEEE.

Tai, W. T. (2006). Effects of training framing, general self-efficacy and training motivation on trainees' training effectiveness. Personnel review, 35(1), 51-65.

Timms, K. 2017. BYOD must be met with a wider appreciation of the cyber-security threat. Computer Fraud & Security 7:5-8.

Velzian B. How to create a Bring Your Own Device (BYOD) policy. Wandera. 2021. https://www.wandera.com/how-to-create-a-bring-your-own-device-byod-policy.

Yim, MS (2021). Security Policy Compliance Motivation: From Technology Threat Avoidance Perspective. Digital Convergence Research, 19(11), 327-339.

저자소개

이창근 육군사관학교 경영학과를 졸업하고, 연세대학교 산업공학과에서 석사과정에 재학 중이다. 주요 관심분야는 기술경영, 품질경영, 경영정보시스템(MIS)이다.

유준우 연세대학교 산업공학과를 졸업하고, 동대학원에서 박사과정을 졸업하였다. 주요 관심분야는 기술경영, 안전관리, 소비자행동 분석 및 의사결정이론 등을 기반으로 한 전략수립 및 가이드라인 개발 등이다.

박준성 연세대학교 산업공학과를 졸업하고, 동대학원에서 박사과정을 졸업하였다. 주요 관심분야는 고객 리뷰 데이터를 활용한 서비스 품질 및 고객 이탈이다. PLS-SEM, Hayes process macro, 자연어 처리 등 다양한 방법론을 활용한다. 이러한 다양한 접근 방식을 통해 서비스 품질 평가와 고객 이탈의 이해를 심화하고자 한다.

조영주 네브라스카 주립대에서 경영학사와 데이터 분석 석사 과정 졸업하고, 연세대학교 산업공학과에서 박사과정에 재학 중이다. 주요 관심분야는 기술경영, 조직관리이다.

유준영 인천대학교 산업경영공학과를 졸업하고, 연세대학교 산업공학과에서 석박사 통합과정에 재학 중이다. 주요 관심분야는 기술경영, 마케팅 전략이다.

김소영 아주대학교 산업공학과 학사를 졸업하고, 연세대학교 산업공학과에서 석사과정에 재학 중이다. 주요 관심분야는 특허분석, 기술경영이다.

박희준 George Washington University에서 공학경영 전공으로 박사학위를 취득하고 Marymount University 경영학과에 재직하였으며, 현재 연세대학교 산업공학과에 재직 중이다. 주요 관심 분야는 플랫폼 기반의 혁신 전략, 비즈니스 모델 개발, 전략 수립 및 성과평가 방법론 개발 등이다.