BYOD SECURITY POLICY COMPLIANCE IN MALAYSIAN PUBLIC UNIVERSITIES: AN INTEGRATED PMT –TPB – GDT MODEL WITH ISA MODERATION

Odai Ali Ali Sharfadeen[1] , Azah Anir Norman[2*], Norjihan Abdul Ghani[3]

[1]Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[2]Information System Department, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[3]Information System Department, Faculty of Computer Science & Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

Emails: nw.odai22@gmail.com[1] , s2102543@siswa.um.edu.my[1], azahnorman@um.edu.my[2*], norjihan@email.edu.my[3]

ABSTRACT

The Bring Your Own Device (BYOD) initiative is widely implemented across various organizations today. Numerous universities in Malaysia are also adopting this approach since it reduces expenses related to maintenance and device management. This paper proposes a framework to enhance compliance with BYOD security policies in the public sector. It identifies the key factors influencing user compliance and contributes to the development of a comprehensive BYOD security policy compliance framework. Quantitative data collection was conducted in Malaysian public universities to examine user behaviors and empirically test the proposed framework. The validation process with experts was executed, and consent was received to participate in the evaluation stage. The findings confirm the effectiveness of integrating (PMT), (GDT), and (TPB) Theories in shaping compliance. All examined variables—including perceived severity, perceived threats, response efficacy, self-efficacy, and formal sanctions—were found to significantly influence attitudes, subjective norms, and behavioral control, which directly affect users' intentions to comply. Information security awareness was validated as a moderator of both attitude and intention to comply. Overall, this study provides empirical validation of the proposed BYOD framework and offers actionable guidance for policymakers, enabling universities to mitigate BYOD related risks, strengthen compliance, and safeguard credibility amid digital transformation.

Keywords: BYOD security compliance; BYOD behavioral framework; BYOD in public universities; Information Security Awareness; BYOD risks and factors; Higher Education BYOD compliance behavioral framework.

1.0 INTRODUCTION

The term Bring Your Own Device (BYOD) refers to a cybersecurity practice in which organizations permit employees to access institutional resources and perform work-related tasks using their personal devices [1]. Although BYOD enhances convenience and productivity, it simultaneously introduces significant security risks, as personal devices may inadvertently host malicious programs without the user's awareness of the potential consequences [2]. During the COVID-19 pandemic, more than 82% of organizations adopted BYOD policies, enabling both employees and institutions to leverage personal devices for work-related activities [3]. A survey of 2,000 organizations revealed that BYOD policies were implemented in 19% of them, with 45% of users employing their personal devices in the workplace [4]. Many organizations that adopted BYOD policies reported that these policies were as effective as those applied to company-owned devices [5].

To ensure effective implementation, organizations must adopt critical management approaches, techniques, and procedures—such as managing networks, mobile devices, mobile applications, mobile information, and corporate mobility—whenever BYOD policies are introduced to regulate device use in the workplace [6]. Within this context, behavioral intention is defined as the degree to which an individual intends to engage in a particular behavior [7]. BYOD users should therefore be aware of the components of the security policy and understand the requirements necessary for compliance [8]. More broadly, behavior refers to the actions or reactions of individuals in response to external or internal motivations, often guided by attitudes, beliefs, and social norms [9], [10]. In the

context of security compliance, behavior is typically understood as the extent to which individuals adhere to or deviate from prescribed security policies and procedures, influenced by factors such as awareness, motivation, and perceived organizational support [1], [11].

Behavioral aspects of security compliance models encompass the psychological and social dimensions that drive individual decisions to follow security guidelines, making them a critical factor in the design of effective security policies [12], [13]. These behaviors are shaped not only by personal attitudes but also by the environmental and organizational contexts in which individuals operate [14], [15]. In Malaysia, for example, the implementation of BYOD models must consider the cultural and social behaviors of university staff and students, ensuring that security awareness programs align with behavioral principles [15]. Effective models often combine technical and behavioral strategies to enforce compliance, since reliance solely on technological solutions may be insufficient [16].

Adoption studies emphasized the role of individual attitudes, contextual factors, and behavioral intentions in shaping BYOD use [1], [4], [14]. In contrast, BYOD enforcement studies underscore the necessity of institutional policies, technical safeguards, and compliance mechanisms to mitigate organizational risks [5], [6], [8]. This distinction highlights the evolution of BYOD from informal, employee-driven practices to structured organizational governance, a transformation that was particularly accelerated during the COVID-19 pandemic.

Building on this perspective, many studies recommended the development of practical efficacy models of BYOD policy compliance to serve as guidelines [13], [17], [18]. Failure to comply with policies may stem from user attitudes, and organizations have emphasized the need for greater understanding of BYOD security's impact on information security and associated risks [10], [19]. A study conducted across 20 public Malaysian institutions of higher learning uncovered relevant theories of BYOD security policy and proposed a reference model that can be adapted to create a comprehensive security policy for Malaysia's educational sector [20].

Research on enhancing compliance has focused on techniques and procedures designed to improve individuals' psychological responses to organizational security policies [21], [22]. Meanwhile, studies on non-compliance have proposed strategies for reducing irresponsible behaviors, as demonstrated in [23]. Strengthening organizational data security is therefore essential in the context of BYOD [24]. However, Protection Motivation Theory (PMT), the Theory of Planned Behavior (TPB), and General Deterrence Theory (GDT) have rarely been integrated into a single conceptual model to study users' security behavior toward BYOD [25], [26], [27], [28].

1.1 Problem Statement

The Bring Your Own Device (BYOD) policy provides flexibility and cost savings for both organizations and employees, but it also exposes critical data to serious security threats [6]. Risks such as malware, device theft, and social engineering attacks can enable unauthorized access to organizational networks and sensitive information [2]. A lack of user awareness and limited compliance with Information Security Policies (ISPs) remains a major challenge, often shaped by user attitudes and insufficient understanding of BYOD-related risks [10], [19] .

Although some universities have established information security policies and implemented training programs, Malaysian higher education institutions continue to face difficulties in achieving effective implementation and compliance [20] . A cross-cultural empirical analysis examined whether cultural factors influence ISP compliance in Malaysian universities, and the findings confirmed that security awareness significantly shapes user perceptions [13], [9]. Several studies have recommended the development of integrative models that combine theoretical frameworks with contextual factors to strengthen user compliance with information security policies, particularly in the public sector [18] , [13]. Designing novel model constructs is therefore vital to mitigate insider threats and safeguard information assets across institutions [11]. To address these challenges, this study proposes a hybrid compliance model that integrates Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and the Theory of Planned Behavior (TPB). The model aims to enhance user compliance, protect organizational data, and provide a guideline for developing effective BYOD security policies in the public sector.

1.2 Research Objectives

Several objectives have been formulated as follows to achieve the research aims:

RO1: To identify factors influencing BYOD security policy compliance behavior among users.

RO2: To develop a BYOD Security Policy Compliance Behavioral Model for the top universities.

RO3: To validate the BYOD Security Policy Compliance Behavioral Model.

2.0 LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

In the literature, researchers have employed several approaches to conceptualize and operationalize theories concerning BYOD compliance in public universities. Prior studies have demonstrated the significance of PMT, TPB, and GDT as foundational frameworks for understanding security behaviors. Accordingly, this study proposes

an integrated model comprising PMT, TPB, and GDT constructs to explain the factors influencing users' security behavior in a developing compliance, as summarized in Table 1 and depicted in the research framework in Fig. 1.

Table 1: Most Impact Theories on ISPC

No	Theories	Limitation	Authors
1	Protection Motivation Theory (PMT)	The lack of social norms undermines compliance [19], and accurate risk assessment remains inherently complex [30].	[1], [15], [16], [17], [19], [25], [26], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [60], [64], [65], [68], [71], [72], [73], [74], [79], [80], [81], [83], [84], [86], [87], [88], [89], [93], [96], [98], [99], [110], [113]
2	Theory of Planned Behavior (TPB)	The model is complex and does not accurately capture the factors driving actual behavior [30].	[1], [12], [17], [32], [41], [46], [47], [48], [49], [50], [51], [52], [53], [54], [60], [71], [72], [73], [77], [83], [90], [93], [95], [96], [99], [107], [109], [110], [113]
3	General Deterrence Theory (GDT)	There is a lack of comprehensive understanding of interconnected criminal activity [19].	[16], [19], [22], [35], [39], [41], [52], [54], [55], [56], [57], [58], [59], [61], [62], [72], [73], [77], [88], [93], [99], [100]

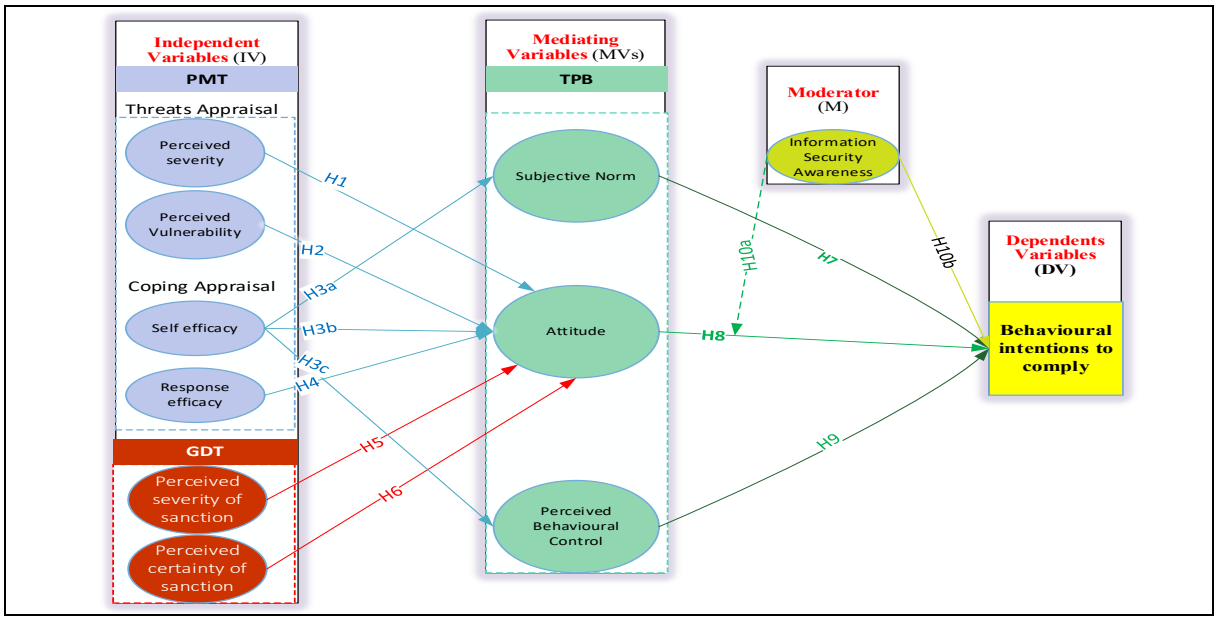

Fig. 1: Research Framework

2.1 Protection Motivation Theory (PMT)

An efficient framework for examining changes in user security behavior has been widely recognized [36], [37], [68]. Prior studies indicate that faculty members' perceptions of the benefits of compliance significantly influence their willingness to adopt security measures [63], [64], [65]. Applying Protection Motivation Theory (PMT) to BYOD compliance among university staff, researchers found that a higher perceived threat of data breaches and stronger beliefs in the effectiveness of adhering to BYOD policies are positively associated with compliant behavior [8]. Accordingly, PMT constructs—perceived threat severity, perceived threat vulnerability, self-efficacy, and response efficacy—can be integrated into a unified model to encourage BYOD compliance [64], [65], [110], [112].

2.1.1 Perceived Threat Severity

Perceived severity and threats are essential constructs as they shape individuals' understanding of the potential risks associated with information security policies [16], [42], [47], [64], [65], [68], [71], [72], [73], [80], [83]. [84], [87], [88], [89], [93], [98]. [99], [112].

H1 ***Perceived Threat Severity positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

The relationship between perceived threat severity and users' attitudes toward information security policies is well established, as researchers have consistently demonstrated that perceived threat severity is a critical factor in fostering positive attitudes toward compliance [16], [42], [47], [66] , [71], [72], [73], [99]. Evidence further reinforces the notion that when users perceive a significant threat, they are more likely to develop favorable attitudes toward adhering to security guidelines [72], [73]. A study found that participants who perceived greater severity of potential security breaches demonstrated more positive attitudes toward compliance, a relationship consistently supported by empirical evidence showing a strong correlation between perceived threat severity and users' attitudes toward adherence to information security policies [68], [99].

2.1.2 Perceived Threat Vulnerability

Perceived threat vulnerability refers to a user's belief that they may experience adverse consequences when engaging in risky behaviors [16], [42], [47], [64], [65], [66], [67], [68] , [69], [71], [72], [73], [79], [80], [81], [84], [86], [87], [88], [89]. Prior research has consistently identified perceived vulnerability as one of the most predictive indicators positively associated with intentions to comply with information security policies among university staff and faculty [1], [15], [33], [42], [45], [69], [74], [83], [93]. [96], [98], [99], [110], [112].

H2 ***Perceived Threat Vulnerability positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

Perceived threat vulnerability is therefore recognized as a critical factor influencing attitudes toward compliance. A cross-sectional study among university students revealed that individuals who perceived higher levels of data security threats were more inclined to adopt positive attitudes toward compliance with BYOD policies [66], [82], [99]. Moreover, several studies have confirmed that perceived vulnerability significantly shapes compliance behaviors, reinforcing its role as a key determinant of adherence to information security policies [16], [71], [73].

2.1.3 Self-Efficacy

A study conducted among Kenyan university students found that self-efficacy had a significant relationship with behavioral intention [51]. Self-efficacy has consistently been shown to exert a positive impact on the intention to comply with information security policies [1], [47], [63], [65], [64], [68], [74], [75], [76], [79], [80], [81], [83], [86], [87], [88], [89], [93], [93], [94], [98]. [99], [110], [112].

H3a ***Self-Efficacy positively affects users' subjective norms toward behavioral intentions to comply with information security policies.***

Self-efficacy also significantly influences subjective norms, which reflect the perceived social pressure to comply with expectations regarding information security policies [18], [109], [110], [112]. In addition, self-efficacy plays a crucial role in shaping users' attitudes toward compliance. Several studies focusing on faculty members have identified that higher levels of self-efficacy among educators were associated with more positive attitudes toward integrating personal devices into the learning environment [8].

H3b ***Self-Efficacy positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

Students with greater self-efficacy exhibited more favorable attitudes toward using their own devices for academic purposes [18]. Moreover, researchers have shown that higher self-efficacy not only directly increases users' intentions to comply but also indirectly strengthens those intentions by enhancing attitudes. This positive association between self-efficacy and attitude has been further confirmed by empirical studies [47], [73], [82].

H3c ***Self-Efficacy positively affects users' perceived behavioral control toward behavioral intentions to comply with information security policies.***

Higher levels of self-efficacy amplify individuals perceived control over their actions, thereby enhancing their intention to comply with security policies [16], [18], [71].

2.1.4 Response Efficacy

Response efficacy refers to the proper and efficient protective behavior undertaken in the face of threats, risks, or vulnerabilities that may lead to privacy loss. It has been identified as one of the most predictive indicators positively associated with intentions of information security compliance among university staff and faculty [11]. Recent research has proposed that enhancing individuals' confidence in the effectiveness of their compliance actions can contribute to greater adherence [79]. Specifically, studies have demonstrated that individuals who believed adherence to BYOD policies would effectively mitigate security risks were more likely to exhibit stronger intentions to comply [15], [31], [36], [64], [65], [68], [76], [80], [82], [83], [84], [86], [87], [88], [89], [93], [96]. [98], [99], [107], [110], [112].

H4 ***Response Efficacy positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

Response efficacy—defined as the belief in the effectiveness of recommended actions to prevent or mitigate security threats—represents a critical factor influencing attitudes toward compliance [16], [66], [72], [73], [77], [82].

2.1.5 Response Cost

Response cost refers to the perceived burden or expense incurred by users when engaging in protective behaviors. Although this factor has been measured in numerous studies, findings consistently indicate that it exerts an insignificant effect on individuals' intentions to comply with information security policies (ISPs) [36], [44], [45], [68], [69], [80], [85]. Consequently, many researchers have excluded response cost from their models, aligning with the broader consensus in the literature such as the result in UK confirmed that response cost insignificant influence toward to intention to comply [93], [98]. [99], [110], [112].

2.2 General Deterrence Theory (GDT)

Perceived formal sanctions refer to individuals' perceptions of the official consequences or punishments imposed by an organization or authority for violating information security policies or engaging in risky behaviors [12], [17], [18], [22], [24], [32]. Such consequences may include loss of reputation, competitive advantage, productivity, and profit, resulting from behaviors that threaten the availability, confidentiality, and integrity of organizational information assets [44], [93]. These perceptions of formal sanctions—whether academic, professional, or legal—are widely recognized in the literature as critical factors influencing compliance with information security policies [41], [48], [55], [57], [59], [61], [62], [72], [100], [106], [112]. Within the framework of (GDT), perceived formal sanctions are typically divided into two dimensions: perceived severity of sanctions and perceived certainty of sanctions [73], [77], [88].

2.2.1 Perceived Severity Sanctions

Perceived severity refers to a user's belief about the seriousness of the punishment they will face if they violate BYOD policies [103]. Users who perceive sanctions as severe are more likely to comply with organizational policies [59], [93], [100], [112].

H5 ***Perceived Severity of Sanction positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

The perceived severity of sanctions—including academic penalties, restricted access to resources, or legal actions—can significantly shape individuals' attitudes toward compliance [11], [23], [56], [57], [58], [59], [72], [99], [103]. Beyond influencing attitudes, perceived severity also functions as a deterrent against non-compliant behavior, reinforcing adherence to organizational security policies.

2.2.2 Perceived Certainty Sanctions

Perceived certainty of sanctions reflects the extent to which individuals believe they will be punished if they fail to comply with prescribed security policies [73]. To strengthen compliance, organizations must clearly communicate both the severity and certainty of sanctions through training sessions, awareness campaigns, and transparent policy guidelines [48], [50], [55], [58], [59], [93].

H6 ***Perceived Certainty of Sanction positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

The relationship between perceived certainty of sanctions and compliance is grounded in deterrence theory, which posits that the likelihood of sanction enforcement strongly influences individual behavior [68]. Empirical studies consistently demonstrate a positive correlation between perceived certainty of sanctions and users' attitudes toward compliance with BYOD policies [11], [23], [56], [57], [58], [59], [72], [99], [103].

2.3 Theory of Planned Behavior (TPB) as Mediator Factors

(TPB) offers a robust framework for understanding how subjective norms, attitudes, and perceived behavioral control shape individuals' intentions and subsequent behaviors. Within the higher education BYOD context, TPB enables the exploration of students' and educators' attitudes toward using personal devices for learning, the influence of peer and institutional norms, and the perceived ease or barriers associated with technology use [65]. Numerous studies have demonstrated that attitudes can mediate the effect of external interventions on behavioral intentions [60], [71], [77].

2.3.1 Subjective Norms

Subjective norms refer to the influence of an individual's social environment on behavior [1], [32], [77], [90], [93].

H7 ***Subjective Norm positively affects users' behavioral intentions to comply with information security policies.***

The mediating role of subjective norms in the relationship between self-efficacy and behavioral intentions has been well established. Subjective norms serve as a significant mediating mechanism through which perceived severity, perceived threats, self-efficacy, and response efficacy positively impact compliance intentions [1], [16], [17], [18], [25], [32], [35], [41], [46], [49], [52], [57], [59], [63], [71], [72], [82], [83], [95], [96], [99], [103], [104], [107], [109], [110], [112].

2.3.2 Attitude

Attitude refers to the evaluation of behavior based on its expected outcomes, whether desirable or unfavorable [1], [12], [17], [29], [30], [48]. Attitude has been shown to significantly influence the adoption of information security policies among users[1], [25], [32], [60], [63], [90], [93], [95], [104], [107], [108], [109], [110],

H8 ***Attitude positively affects users' behavioral intentions to comply with information security policies.***

The mediating role of attitudes in the relationship between perceived threat severity and behavioral intentions is well documented. Findings indicate that attitudes serve as a critical mechanism through which perceived severity, perceived threats, self-efficacy, and response efficacy positively influence compliance intentions [1], [12], [16], [17], [21], [30], [32], [37], [41], [42], [48], [51], [57], [59], [60], [66], [71], [72], [73], [82], [83], [95], [99], [103], [112]. Moreover, attitudes have been found to fully mediate the impact of formal sanctions on ISP behavioral intentions [23].

2.3.3 Perceived Behavioral Control

Perceived behavioral control refers to the extent to which individuals believe they can regulate or manage behaviors of importance. Empirical evidence showed that perceived behavioral control significantly influences behavioral intention [1] and has a positive impact on compliance with information security policies [23].

H9 ***Perceived Behavioral Control positively affects users' behavioral intentions to comply with information security policies.***

Researchers have demonstrated that enhancing individuals' perceived control over following BYOD security protocols increases compliance rates [96]. Perceived behavioral control has consistently been shown to positively affect users' behavioral intentions to comply with information security policies [1], [12], [17], [18], [19], [24], [32], [41], [48], [57], [63], [71], [72], [77], [99], [104], [112].

2.4 Information Security Awareness (ISA) as Moderator Factor

(ISA) is defined as the extent to which users understand the importance of information security policies, rules, and regulations, and take responsibility for protecting organizational information by acting accordingly [25]. Developing a well-structured training and awareness program is therefore essential for organizations. Active

participation in such programs ensures effectiveness and provides clear guidelines for policy development and compliance [77], [79], [94], [102], [105], [112].

H10a ***Information Security Awareness positively affects users' attitudes toward behavioral intentions to comply with information security policies.***

Attitude plays a pivotal mediating role in the relationship between ISA and users' intentions to comply with security policies [17], [32], [42], [47], [60], [74], [95], [99], [106], [108], [109]. ISA has been identified as a critical factor influencing user behavior in leading universities and higher education institutions. Empirical evidence confirmed that ISA positively shapes users' attitudes toward compliance intentions [99].

H10b ***Information Security Awareness positively affects users' behavioral intentions to comply with information security policies.***

Studies consistently demonstrated that ISA plays a crucial role in shaping individuals' behaviors toward compliance with security policies [1], [8], [32], [47], [50], [51], [53], [60], [63], [65], [67], [72], [77], [82], [86], [92], [99], [102], [103], [109], [112]. By increasing awareness, organizations can strengthen both attitudes and behavioral intentions, thereby improving adherence to information security policies [91], [105] .

2.5 PUBLIC UNIVERSITIES AND BYOD COMPLIANCE STATUS

Researchers have reported that most students prefer using their personal devices for academic and significant positive influence on the academic performance of students [70].Researchers requested to give organizations a better awareness of how to create more model personal device policies among students [81], [102]. Leading universities are adapting to this trend by implementing policies that encourage BYOD adoption while simultaneously addressing security concerns. The integration of PMT, TPB, and GDT provides a comprehensive framework for understanding and enhancing BYOD compliance in public universities [27]. Current efforts focus on implementing strategies and developing BYOD frameworks that align with educational agendas, aiming to strengthen information security protection and reduce risks across campus environments [20], [70].

Insufficient Malaysian higher education universities have developed comprehensive information security policies to educate faculty, staff, and students about the importance of information security and to promote a culture of security-conscious behavior through information security awareness, but the results confirmed that there is a lack in sound implementation and compliance of information security policies in the higher education sector [113].In the academic community, BYOD users should have enough knowledge of their accountability and integrity in every action they take to prevent any loss to the organization through the BYOD practice, potential attacks that might cause the universities in loss if BYOD security policy is launched without having a robust model to refer of its components [20]. The issue is further complicated by differences in compliance behaviors among academic staff, administrative staff, and students. Academic staff often demonstrate higher resistance to compliance, citing perceived autonomy and concerns that security measures may hinder academic freedom [10], [11]. This perception contributes to lower compliance rates [26]. In contrast, administrative staff—who typically handle sensitive information—tend to be more compliant due to heightened awareness of the consequences of data breaches [15]. Students, meanwhile, are generally more compliant because of the structured nature of their roles and their greater awareness of the risks associated with non-compliance [37], [49], [73], [110]. A case study in Malaysian higher education confirmed that cultural values such as ISA toward security compliance, but weak institutional enforcement reduces overall effectiveness [107].

2.5.1 Previous Related Frameworks

Prior research has consistently confirmed the efficacy of integrating (PMT), (TPB), and (GDT) in explaining individuals' behavioral intention to comply. These models within academic environments are practical insights into the factors shaping compliance behavior. In this study, several existing frameworks have been adapted to guide the development of a more comprehensive framework, one that builds upon established theoretical foundations while incorporating critical contextual factors.

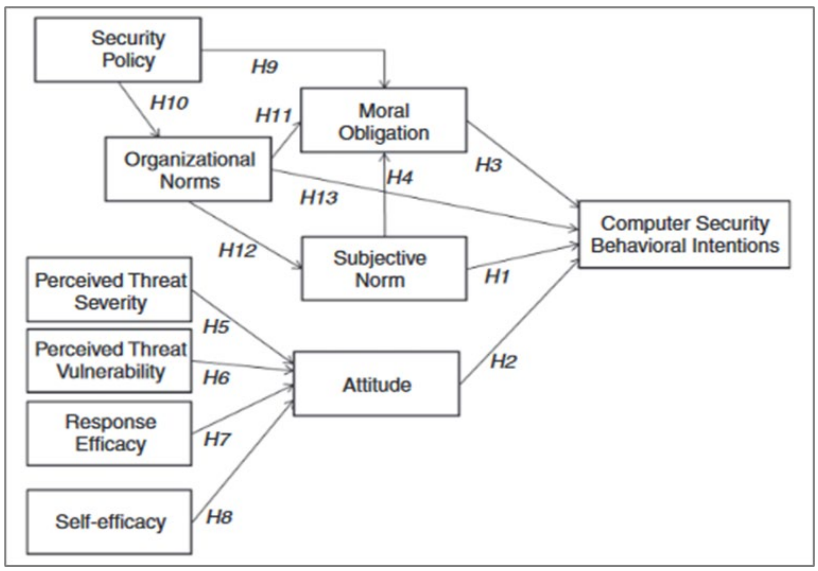

Fig. 2: Model of Understanding Computer Security Behavioral Intention in the Workplace: An Empirical Study of Korean Firms [7]

Fig. 2. The framework integrated PMT and the TPB to assess intentions to comply with information security policies. The results showed that perceived threat vulnerability and severity significantly shape users' attitudes toward compliance; self-efficacy exerts a positive effect on subjective norms, attitudes, and perceived behavioral control; and response efficacy further strengthens attitudes in favor of compliance. These findings underscored the joint influence of internal cognitive factors and external normative and threat-related factors in determining compliance behavior [7].

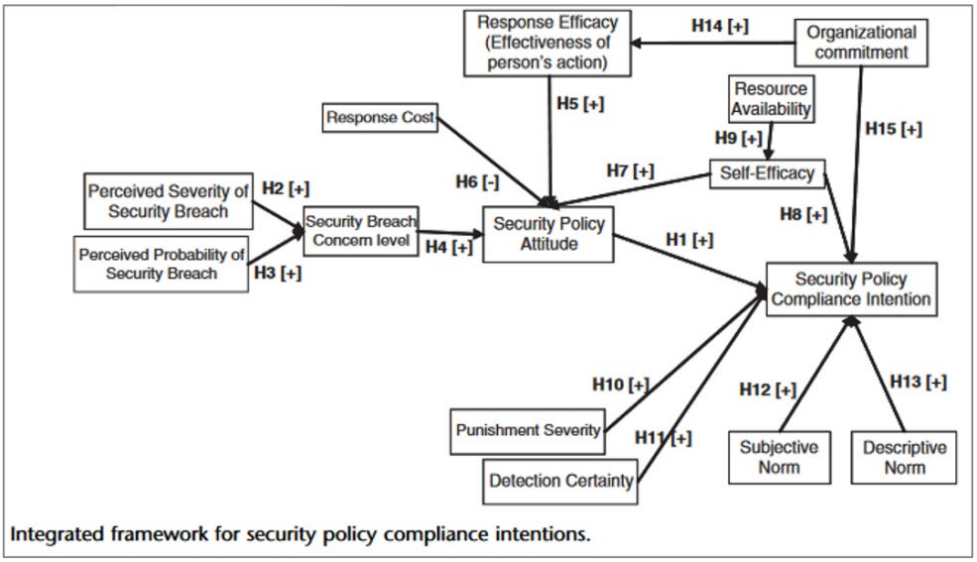

Fig. 3: Protection Motivation and Deterrence: A Model for Security Policy Compliance in Organizations [73]

Fig. 3. This framework utilized theoretical models such as Organizational Commitment, (PMT), (TPB), and (GDT) to assess key factors influencing users' intentions to comply with information security policies. the results confirmed that Response cost had no effect on attitude, while perceived threat severity, threat vulnerability, response efficacy, and self-efficacy had strong effects on attitudes. Subjective and descriptive norms positively influenced users' intentions, and perceived formal sanctions, also impacted user intentions [73].

2.5.2 Hypotheses of Research Framework

All hypotheses of the proposed model have been supported by previous studies; authors are presented in Table 2.

Table 2: Hypotheses of Research

H(n)	Hypotheses	Authors
H1	PTS(+)→ATT	[16], [42], [47], [71], [72], [73], [82], [99]
H2	PTV(+)→ATT	[16], [42], [47], [66], [71], [72], [73], [82], [99]
H3a	SE(+)→SN	[18], [110]
H3b	SE(+)→ATT	[47], [73], [82]
H3c	SE(+)→PBC	[16], [18], [71], [99]
H4	RE(+)→ATT	[16], [66], [72], [73], [82]
H5	PSS(+)→ATT	[11], [23], [56], [57], [59], [72], [103]
H6	PCS(+)→ATT	[11], [23], [56], [57], [59], [72], [103]
H7	SN(+)→BI	[1], [16], [17], [18], [30], [32], [35], [41], [46], [49], [52], [57], [59], [63], [71], [72], [77], [82], [83], [93], [95], [96], [99], [103], [104], [107], [109], [110], [111], [112]
H8	ATT(+)→BI	[1], [12], [16], [17], [21], [29], [30], [32], [34], [37], [41], [42], [48], [51], [57], [59], [63], [66], [71], [72], [73], [82], [83], [93], [95], [99], [103], [104], [106], [109], [108], [110], [112]
H9	PBC (+)→BI	[1], [12], [17], [18], [19], [24], [32], [41], [48], [57], [71], [72], [95], [99], [104], [106], [112]
H10a	ISA(+)→ATT	[17], [32], [42], [47], [74], [95], [99], [103], [106], [108], [109]
H10b	ISA(+)→BI	[1], [47], [32], [50], [82], [51], [52], [53], [63], [65], [67], [72], [77], [99], [101], [102], [103], [105] , [112]

3.0 METHODOLOGY

This study employs a survey method with a quantitative research design to explore users' actual behaviors in depth. This approach enables the collection of comprehensive data for generalization across the target population. The flow chart for this research's methodology is shown in Fig. 4.

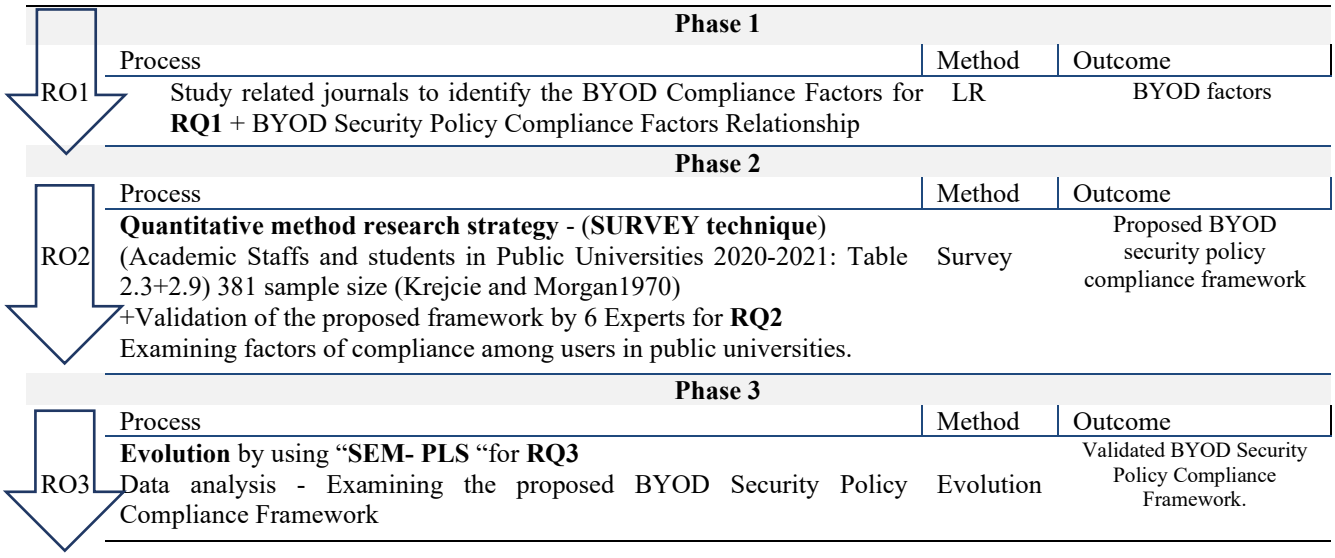

Fig. 4: Research Design

3.1 Data collection method and Sample size

The target sample of this study is the public sector. So, our study will distribute the survey among academic staff, management staff, and users/students to identify all behaviors among users 380 as a sample size for Malaysia's top five public universities. The unit of analysis was a user who complies with information security policy with their own devices used. The technique is probability sampling.

3.1.1 Sample Process

The sample data were collected from the top five public universities in Malaysia which are Universiti Malaya (UM), Universiti Putra Malaysia (UPM), Universiti Kebangsaan Malaysia (UKM), Universiti Sains Malaysia (USM), and Universiti Teknologi Malaysia (UTM). Three groups were categorized after a simple statistical sample process to (academic staff, management staff, and users/students) as BYOD users, the campaign surveys on universities' emails, Facebook groups, and normal distribution. The technique is probability sampling.

3.1.2 Sample size

This study utilized the Considering 5% sample size of five top universities to the latest statistics of Academic Staff and Students in Top universities for 2024: Table 2.3 and Table 2.9 in Appendix B. Inputting these values in a sample size calculator the researchers determined that a sample size of at least 381 would be more suitable to enhance the generalizability of the study's findings, surpassing the minimum sample size indicated by (Krejcie & Morgan, 1970), as shown in Table 3.

Table 3: Minimum sample size

Sample	Population	Sample	Population	Sample	Population
375	15000	254	750	108	150
377	20000	260	800	113	160
379	30000	265	850	118	170
380	40000	269	900	123	180
381	50000	274	950	127	190
382	75000	278	1000	132	200

3.2 Questionnaire Instrument

A questionnaire method was used to collect data from users in top universities (Table 3) to examine their actual behavior when using personal devices for work. 5-point Likert Scale is used to get an accurate result, as shown in Appendix A.

3.3 Experts Validation and Confirmation of the Framework

This validation process is of critical importance to this study, as all participating experts, who possess extensive experience and expertise relevant to the field, have provided their consent to serve as experts validation (Table 4).

Table 4: Experts Validation and Confirmation of the Framework

Expert	Organization	Comments/Modifications	Validation by expert
Expert 1 - Academic	Top university 1	ISA is also part of education	This proposed framework is excellent, with the intent of improving ISA.
Expert 2 – Industry	Local Cybersecurity company 1	Some items of the survey have been modified.	Overall, it is an excellent proposed framework.
Expert 3 – Industry	Local Cybersecurity company 2	Some items of the survey have been modified.	Validated.
Expert 4- Industry	Government Sector	make it simpler to introduce your theory and questions.	Validated
Expert 5- Academic	Public university 2	Some items of the survey have been modified.	Validated.
Expert 6- Academic	Public university 3	Some items of the survey have been modified.	Validated.

4.0 Findings

This section presents the demographic characteristics of the respondents and provides a descriptive analysis of the latent constructs, highlighting the distribution, central tendency, and variability of the measured variables.

4.1 The Respondents' Demographic Profile

Based on face-to-face survey distribution, along with follow-up reminders through calls and emails sent to individuals, groups, academic departments, and university management personnel, a total of 400 questionnaires were distributed, of which 360 were successfully collected, as shown in Table 5.

Table 5: The Respondents' Demographic Profile

Demography	Description	No. responses	%
Gender	Female	197	54.72
	Male	158	43.88
	Prefer not to say	5	1.38
Age	20-29	93	25,83
	30-39	128	35.55
	40-49	95	26.38
	above 50	44	12.22
Highest level of education	Bachelor	105	29.16
	Master	123	34.16
	PhD	132	36.66
What type of organization do you belong to?	Public Company	1	0.27
	Public Corporation	2	0.55
	Public University	357	99.16
What is your position?	Academic Staff	201	55.83
	Management	53	14.72
	User/Student	106	29.44
Are you using your own devices for working purposes at the workplace or remotely?	No	0	0
	Yes	360	100
How many years have you been using your devices for working purposes?	0-5	30	8.33
	6-10	330	91.66

4.2 Descriptive Analysis of Latent Construct

Descriptive statistics were applied to summarize the study constructs, including independent, moderating, mediating, and dependent variables. Table 6 presents the maximum, minimum, mean, and standard deviation (SD) values based on a five-point Likert scale (1–5). The mean scores ranged from 2.01 to 2.13, with SD values between 0.48 and 0.56. Mean scores below 3.00 were classified as low, 3.00–5.00 as moderate, and above 5.00 as high.

Table 6: Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
PTS	360	1.00	3.33	2.0616	.55854	-.127	.134	-.845	.268
PTV	360	1.00	3.67	2.0697	.53344	.138	.134	-.592	.268
SE	360	1.00	3.33	2.0747	.53117	-.122	.134	-.671	.268
RE	360	1.00	3.67	2.0253	.53927	.128	.134	-.333	.268
ATT	360	1.00	3.33	2.0222	.52513	.054	.134	-.821	.268
SN	360	1.00	3.33	2.0182	.53295	.108	.134	-.582	.268
PBC	360	1.00	3.67	2.1323	.50295	-.258	.134	-.237	.268
PSS	360	1.00	3.33	2.0929	.52956	.029	.134	-.734	.268
PCS	360	1.00	3.33	2.1232	.51813	-.280	.134	-.701	.268
ISA	360	1.00	3.20	2.0618	.48622	-.116	.134	-.669	.268
BI	360	1.00	3.33	2.0808	.56481	-.132	.134	-.664	.268

5.0 RESULTS

The PLS-SEM 4.0.2.1 approach was employed to analyze the direct, mediating, and moderating relationships among the constructs after all validity tests [97]. All results are validated by internal consistency, composite reliability, correlation and discriminant validity as following in Table 7 and Fig. 5.

Table 7: Discriminant Validity (Fornell Larcker)

Fornell Larcker	ATT	BI	ISA	PBC	PCS	PSS	PTS	PTV	RE	SE	SN
ATT	**0.848**										
BI	0.710	**0.833**									
ISA	0.508	0.580	**0.805**								
PBC	0.215	0.426	0.323	**0.826**							
PCS	0.611	0.579	0.371	0.304	**0.840**						
PSS	0.561	0.521	0.249	0.078	0.399	**0.821**					
PTS	0.625	0.656	0.368	0.264	0.412	0.355	**0.841**				
PTV	0.687	0.599	0.334	0.180	0.462	0.399	0.475	**0.844**			
RE	0.584	0.521	0.405	0.236	0.374	0.336	0.404	0.420	**0.846**		
SE	0.645	0.640	0.323	0.389	0.490	0.493	0.510	0.450	0.388	**0.844**	
SN	0.468	0.585	0.265	0.069	0.365	0.412	0.345	0.402	0.274	0.377	**0.883**

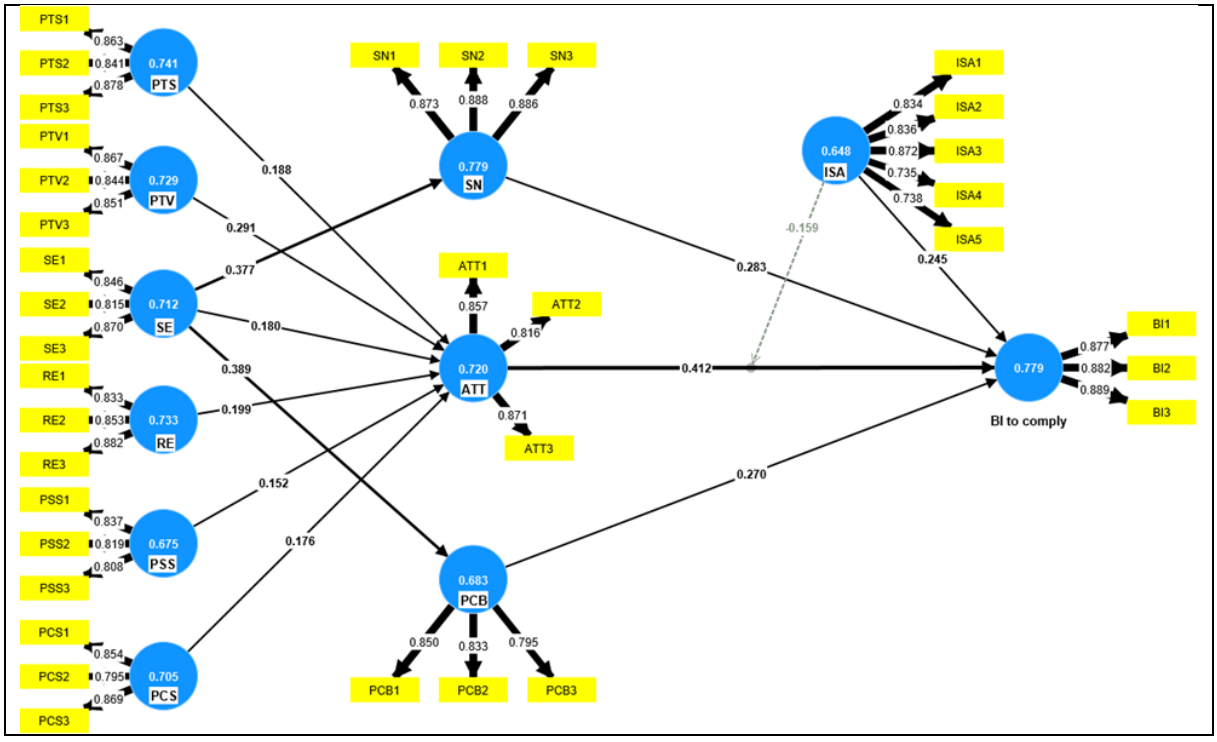

Fig. 5: Structural Model (AVE) & R Square

5.1 Assessment of Hypotheses Relationships

BI conditional on ISA at Mean, positive, and negative according to the data presented in Fig. 6, ISA significantly moderates the relationship between attitude and behavioral intention, showing that the H10a is supported. The researcher assessed the effect sizes of the mediators small, medium, and significant effects, indicated as R, 0.02, 0.15, and 0.35, respectively. The mediators' effect size obtained from smart PLS is presented in Table 8 and Fig.7.

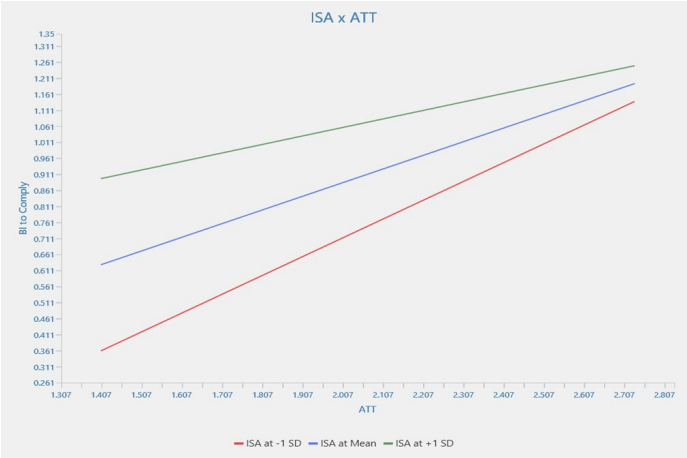

Fig. 6: Effect Size of (F-SQUARE) Direct Moderating Variables

Table 8: Effect Size (R^2) of Excluded Mediators

Mediators	2	2 ex	F-squared	Effect size
SN	0.719	0.643	0.272	Medium
ATT	0.719	0.651	0.277	Medium
PBC	0.719	0.657	0.220	Medium

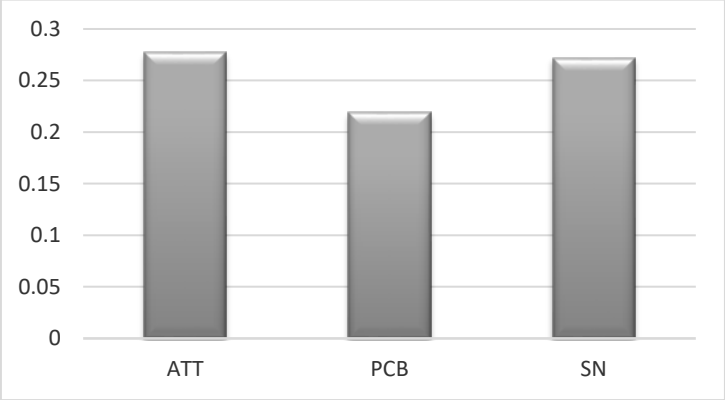

Fig. 7: Effect Size of Excluded Mediators

5.2 Predictive Relevance (Q2)

Q^2 helps determine the relative construct's predictive relevance in an SEM model. In this study, the Q^2 predictive relevance of the PLS path model was tested using a blindfolding procedure with an omission distance of D = 7 by [97]. The guidelines were that if Q^2 is more than zero, the model has predictive relevance; if Q^2 is less than zero, the model does not. The smart-PLS results show that Q^2 of the current study model, which is based on two endogenous constructs named attitude and purchase intention, is greater than zero, indicating that the current study model has predictive relevance (Table 9).

Table 9: PLS Predict All Variables

	SSO	SSE	Q^2 (=1-SSE/SSO)
ATT	1140	652.778	0.427
BI to comply	1140	535.934	0.530
ISA	1900	997.088	0.475
PBC	1140	726.779	0.362
PCS	1140	681.046	0.403
PSS	1140	747.431	0.344
PTS	1140	612.402	0.463
PTV	1140	636.685	0.442
RE	1140	626.686	0.450
SE	1140	668.887	0.413
SN	1140	536.515	0.529

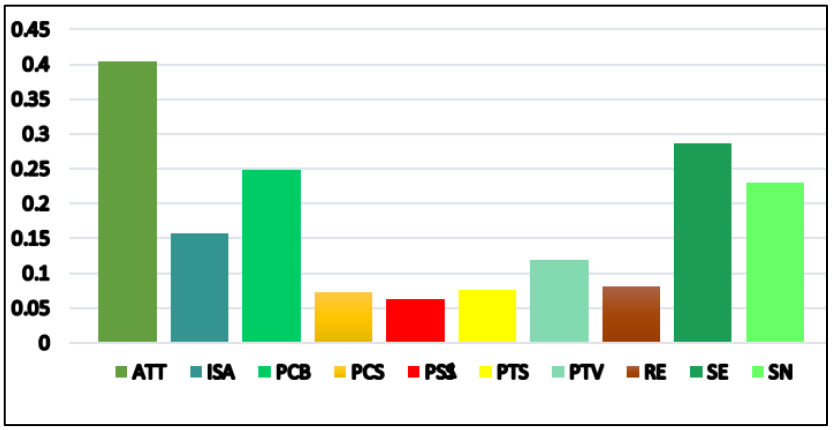

Fig. 8: The Effect Size of All Variables

Fig. 8. Attitude presents the highest effect size (0.44), followed by Self-Efficacy, which demonstrates an effect size of 0.286. Perceived Behavioral Control ranks third, with an effect size of 0.248. Additionally, Self-Efficacy shows an effect size of 0.071 in relation to Attitude.

6.0 DISCUSSION

Compliance is further hindered by uneven policy implementation and resistance among academic staff who perceive security measures as constraints on academic freedom [10]. An experiment at a large public university in the Southwestern United States, involving 189 junior-level management information systems students, showed that perceived threat, perceived severity, self-efficacy, and response efficacy significantly shaped attitudes, while subjective norms and attitudes strongly predicted intentions to comply with information security policies [82]. Complementary evidence indicates that perceived behavior and self-efficacy significantly influence U.S. undergraduates' intentions to adopt information security policies [63]. In Malaysia, a dimension-based information security culture model revealed that hierarchical respect and collective responsibility strongly influence compliance behaviors, yet weak institutional enforcement diminishes overall effectiveness [78], [107]. Perceived threat, self-efficacy, and response efficacy also explain senior managers' failure to implement adequate controls to mitigate data leakage risks in organizations adopting BYOD programs [79].

Comparative studies in Palestinian universities highlighted the role of cultural attitudes toward authority and institutional credibility, mirroring Malaysia's reliance on hierarchical norms and trust [11]. Evidence from Kenyan universities underscored awareness and vulnerability perceptions as critical drivers of compliance, reinforcing the need to embed cultural and awareness dimensions in policy frameworks [51], [53], [102].

Across the United Kingdom, United States, and United Arab Emirates, findings emphasized perceived threat, self-efficacy, response efficacy, attitudes, subjective norms, and deterrence (e.g., certainty and severity of sanctions) as central to compliance, aligning with PMT, TPB, and GDT perspectives [93]. Globally, growing reliance on personal devices for academic and administrative work has driven BYOD adoption, requiring universities to balance flexibility with security [70]. Institutions that integrate PMT, TPB, and GDT into strategy better align security initiatives with educational objectives and mitigate campus-wide risks [27], [55]. Further review reports that 86% of articles identify security issues in IT, 51% in management, 45% in user behavior, and 19% in mobile devices, underscoring the multifaceted nature of compliance challenges [104]. Findings from Saudi universities confirmed that perceived threats, severity, response efficacy, and subjective norms shape intentions to comply, highlighting the importance of culturally tailored policies and training [99]. Overall, the most relevant ISPC frameworks in Table 10 adopt a holistic approach, drawing on the Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), and General Deterrence Theory (GDT) to explain user behavior and strengthen institutional security.

Table 10: Security Policy Compliance Frameworks Comparison

Author	PMT*	TPB*	GDT*	PTS*	PTV*	SE*	RE*	PSS*	PCS*	ATT*	SN*	PCB*	ISA*	BI*
[16]		✓	✓					✓	✓	✓			✓	✓
[73]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
[11]	✓		✓			✓	✓	✓					✓	✓
[47]		✓								✓	✓	✓	✓	✓
[1]	✓	✓		✓		✓				✓	✓	✓	✓	✓
[109]	✓	✓				✓				✓		✓	✓	✓
[7]	✓	✓		✓	✓	✓	✓			✓	✓			✓
[82]	✓	✓		✓	✓	✓	✓			✓	✓	✓		✓
[15]	✓	✓				✓	✓				✓			✓
[6]	✓	✓		✓	✓	✓	✓			✓	✓	✓		✓

* Refer to the abbreviation above

7.0 Ethical Considerations

Regarding the Universiti Malaya Research Ethics Committee (UMREC) with Reference Number: UM.TNC2/UMREC_2095, participants provided informed consent before completing the survey, and participation was entirely voluntary. No personal identifying information was collected, and all responses remained anonymous. Data were securely stored and used solely for academic research in accordance with institutional ethical guidelines.

8.0 Practical Implications

To strengthen BYOD compliance in Malaysian higher education, adopt a structured, multi-layered approach comprising continuous role-specific training with accessible resources, clear and enforceable policies backed by monitoring and formal sanctions for non-compliance, positive reinforcement that frames BYOD as enhancing productivity and data protection with communications leveraging perceived severity, self-efficacy, and response efficacy, and intensified awareness campaigns—especially in public universities—to highlight risks and benefits and foster collective responsibility; Finally, universities should consider the following specific and actionable strategies for universities to improve ISP compliance among students based on these insights. Universities can operationalize the proposed framework and achieve durable improvements in BYOD security compliance.

9.0 Limitations and Future Research

This study is limited by its small sample size, limited to a few Malaysian universities, which restricts the generalizability of the findings. The cross-sectional design further limits causal inference, underscoring the need for longitudinal research to establish temporal relationships among the variables. Future investigations should employ larger and more diverse samples to enhance representativeness and incorporate objective measures—such as direct observation or behavioral assessments—to reduce bias and strengthen validity. Comparative studies across public and private institutions, as well as cross-cultural analyses in different national contexts, would illuminate how organizational and cultural factors shape BYOD compliance. Extending the framework beyond universities to other public sector organizations and conducting long-term evaluations of its effectiveness remain critical avenues for inquiry. Emerging technologies also present promising directions. Blockchain could provide secure, transparent mechanisms for monitoring compliance, while AI and machine learning offer predictive capabilities to identify and mitigate risks of non-compliance proactively. Together, these approaches can advance BYOD policy research by integrating cultural, institutional, and technological dimensions into a comprehensive model of security compliance. Future research could investigate cultural variations in BYOD security compliance across public sector organizations in different countries, such as China, to extend the applicability of the validated framework.

10.0 CONCLUSION

This study emphasizes the significance of information security awareness as a moderator of attitude in improving compliance with BYOD policies in top universities in Malaysia. It highlights the importance of considering (perceived severity, threats, self-efficacy, response efficacy, formal sanctions, subjective norms, attitude, and behavioral control) to develop effective policies that align with users' values and promote compliance as shown in Table 11.

Table 11: Results of Hypotheses

H(n)	Hypotheses	*β* Beta	*SD*	*T*	*P*	Result
H1	PTS -> ATT -> BI	0.083	0.038	2.149	0.032**	Supported
H2	PTV -> ATT -> BI	0.203	0.083	2.444	0.015***	Supported
H3a	SE -> SN -> BI	0.165	0.081	2.049	0.040**	Supported
H3b	SE -> ATT -> BI	0.070	0.032	2.185	0.029**	Supported
H3c	SE -> PBC -> BI	0.178	0.061	2.929	0.003***	Supported
H4	RE -> ATT -> BI	0.111	0.040	2.776	0.006***	Supported
H5	PSS -> ATT -> BI	0.062	0.028	2.188	0.029**	Supported
H6	PCS -> ATT -> BI	0.080	0.037	2.186	0.029**	Supported
H7	SN -> BI	0.229	0.074	3.097	0.002***	Supported
H8	ATT -> BI	0.347	0.102	3.402	0.001***	Supported
H9	PBC -> BI	0.243	0.071	3.447	0.001***	Supported
H10a	ISA -> ATT	0.143	0.054	2.633	0.0143**	Supported
H10b	ISA -> BI	0.234	0.071	3.316	0.001***	Supported

Notes: PTS = Perceived Threat Severity, PTV = Perceived Threat Vulnerability, SE = Self-Efficacy, RE = Response Efficacy, ATT = Attitude, SN = Subjective Norms, PBC = Perceived Behavioral Control, PSS = Perceived Severity of Sanction, PCS = Perceived Certainty of Sanction, ISA = Information Security Awareness, BI = Behavioral Intention to comply; $^{**}p < .05$, $^{***}p < .01$.

By integrating psychological and behavioral constructs for institutions can design policies that resonate with users' values The findings underscore the urgent need for Malaysian higher education to move beyond fragmented initiatives toward comprehensive frameworks that embed security awareness into governance and daily practice. information security awareness plays a pivotal role in shaping attitudes and strengthening compliance with BYOD

policies in Malaysian universities. Effective implementation not only mitigates risks associated with personal device use but also safeguards institutional credibility and the integrity of academic environments.

This research provides actionable insights for policymakers and administrators. Strengthening BYOD compliance is not merely a technical necessity; it is a strategic imperative for ensuring resilience, trust, and sustainable digital transformation across Malaysia's higher education sector.

ACKNOWLEDGEMENT

This work was supported in part by the Ministry of Education (MOE), Malaysia for funding this project with the Fundamental Research Grant Scheme (FRGS) (FP056-2019A) ref-no: FRGS/1/2019/ICT04/UM/02/1.

REFERENCES

[1] Al-Harthy, I M., & Ali, N. A. "Determinants of BYOD protection behavior: An employee's perspective", *Journal of Theoretical and Applied Information Technology*, 100(13), 4653-78, 2022.

[2] Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. "A proposed model for access control in the cloud and BYOD environment", *IJCSNS International Journal of Computer Science and Network Security,* 18(2), 144-152, 2018.

[3] Holger Schulze, "BYOD Security Report," cybersecurity-insiders, Bitglass, San Francisco, USA, Rep., April 2021. 2021 BYOD Security Report [Bitglass] - Cybersecurity Insiders

[4] Alaskar, M. "Understanding contextual factors of bring your own device and user information security behaviors from the work-life domain perspective", *Journal of Information Security,* 12(3), 287-310, 2020.

[5] Bello, A., Murray, D., & Armarego, J. "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments", *Information and Computer Security,* 25(4), 475-492, 2017.

[6] B. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," *2018 1st Int. Conf. on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2018, pp. 1-6, doi: 10.1109/CAIS.2018.8441967.

[7] Yoon, C., & Kim, H. "Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms", *Information Technology & People,* 26(4), 401-419, 2013.

[8] Halim, I. I. A., Buja, A. G., Idris, M. S. S., & Mahat, N. J. "Implementation of BYOD security policy in Malaysia institutions of higher learning (MIHL): an overview", *J. Adv. Res. Appl. Sci. Eng. Technol,* 33, 1-14, 2023.

[9] S. Hina and D. D. Dominic, "Need for information security policies compliance: A perspective in Higher Education Institutions," *2017 Int. Conf. on Research and Innovation in Information Systems (ICRIIS)*, Langkawi, Malaysia, 2017, pp. 1-6, doi: 10.1109/ICRIIS.2017.8002439.

[10] Goh, C. H., & Teoh, A. P. "Determining Bring Your Own Device (BYOD) security policy compliance", *Journal of Information Security and Privacy,* 15(3), 214-230, 2021.

[11] Y. M. Iriqat, A. R. Ahlan and N. N. A. Molok, "Information Security Policy Perceived Compliance Among Staff in Palestine universities: An empirical pilot study," *2019 IEEE Jordan Int. Joint Conf.on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019, pp. 580-585, doi: 10.1109/JEEIT.2019.8717438.

[12] Tam, C., Conceição, C. de M., & Oliveira, T. "What influences employees to follow security policies?", *Safety Science,* 147, 105595, 2022.

[13] Angraini, R. Alinda Alias and O. Okfalisa, "Need for Compliance With Information Security Policy In Universities: a Preliminary survey," *2019 Fourth Int. Conf. on Informatics and Computing (ICIC)*, Semarang, Indonesia, 2019, pp. 1-6, doi: 10.1109/ICIC47613.2019.8985949.

[14] Dang-Pham, D., & Pittayachawan, S. “Comparing intention to avoid malware across contexts in a BYOD enabled Australian university: A protection motivation theory approach”, *Computers & Security,* 48, 281-297, 2015.

[15] Rajab, M., & Eydgahi, A. “Evaluating the explanatory power of theoretical models on intention to comply with information security policies in higher education”, *Computers Security,* 80, 211-223, 2019.

[16] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. “Employees’ intentions toward complying with information security controls in Saudi Arabia’s public organisations”, *Government Information Quarterly,* 39(4), 101721, 2022.

[17] Adam Teoh, A., Binti Abdul Ghani, N., Ahmad, M., Jhanjhi, N., A. Alzain, M., & Masud, M. “Organizational Data Breach: Building Conscious Care Behavior in Incident Response”, *Computer Systems Science and Engineering,* 40(2), 505–515, 2022.

[18] Yeng, P. K., Szekeres, A., Yang, B., & Snekkenes, E. A. “Mapping the Psychosocialcultural Aspects of Healthcare Professionals’ Information Security Practices: Systematic Mapping Study”, *JMIR Human Factors,* 8(2), e17604, 2021.

[19] Palanisamy, R., Norman, A. A., & Mat Kiah, L. “BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts”, *Journal of Organizational Computing and Electronic Commerce,* 31(4), 320–342, 2021.

[20] Ahmed, A. A. A., & Abas, H. “Factors Influencing Information Security Policy Compliance Behavior in High Education Institutions: Systematic Literature Review”, *Advances in Social Sciences Research Journal,* 11(7), 260–273, 2024.

[21] D’Arcy, J., & Lowry, P. B. “Cognitive-affective drivers of users’ daily compliance with information security policies: A multilevel, longitudinal study”, *Information Systems Journal,* 29(1), 43-69, 2019.

[22] Trang, S., & Brendel, B. “A meta-analysis of deterrence theory in information security policy compliance research”, *Information Systems Frontiers,* 21(6), 1265-1284, 2019.

[23] Aurigemma, S., & Mattson, T. “Deterrence and punishment experience impacts on ISP compliance attitudes”, *Information & Computer Security,* 25(4), 421–436, 2017.

[24] Baillette, P., & Barlette, Y. “Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France”, *Journal of Global Information Management,* 28(2), 1–28, 2020.

[25] Barlette, Y., Jaouen, A., & Baillette, P. “Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers’ coping strategies”, *International Journal of Information Management,* 56, 102212, 2021.

[26] Haag, S., Siponen, M., & Liu, F. “Protection Motivation Theory in Information Systems Security Research”, *ACM SIGMIS Database: The Database for Advances in Information Systems,* 52(2), 25–67, 2021.

[27] Ahmadov, S. “Enhancing BYOD mobile device security in a hybrid environment”, *Sustainable Engineering and Innovation,* 5(2), 247–260, 2023.

[28] Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. “Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review”, *Social Sciences,* 11(9), 386, 2022.

[29] Ma, X. “IS professionals’information security behaviors in Chinese IT organizations for information security protection”, *Information Processing Management,* 59(1), 102744, 2022.

[30] Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance", *Applied Sciences,* 11(8), 3383, 2021.

[31] Vrhovec, S., & Mihelic, A. “Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation”, *Computers Security,* 106, 102309, 2021.

[32] Grassegger, T., & Nedbal, D. “The role of users’ information security awareness on the intention to resist social engineering”, *Procedia Computer Science,* 181, 59-66, 2021.

[33] Chen, H., Turel, O., & Yuan, Y. “E-waste information security protection motivation: The role of optimism bias”, *Information Technology People,* 35(2), 600-620, 2021.

[34] Palanisamy, R., Norman, A. A., & Kiah, M. L. M. “Compliance with bring your own device security policies in organizations: A systematic literature review”, *Computers Security,* 98, 101998, 2020.

[35] Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. "Employees’ behavioural intention to smartphone security: A gender-based, cross-national study". *Computers in Human Behavior,* 104, 106184, 2020.

[36] Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). “Using protection motivation theory in the design of nudges to improve online security behavior”, *International Journal of Human-Computer Studies,* 123, 29-39.

[37] Hina, S., Selvam, D. D. D. P., & Lowry, P. B. “Institutional governance and protection motivation: Theoretical insights into shaping users’ security compliance behavior in higher education institutions in the developing world”, *Computers & Security,* 87, 101594, 2019.

[38] Troussard, X., & Van Bavel, R. “How can behavioral insights be used to improve EU policy?”, *Intereconomics,* 53(1), 8-12, 2018.

[39] Ratchford, M., Wang, P., & Sbeit, R. O., "BYOD security risks and mitigations", In *Information Technology-New Generations: 14th Int. Conf. on Information Technology,* 2017, pp. 193-197. Vol 558, Springer, Cham, doi:10.1007/978-3-319-54978-1_27.

[40] Duke Giwah, A. “User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory”, *SoutheastCon,IEEE* 2018, 1–5, 2018.

[41] Nasir, A., Arshah, R. A., & Ab Hamid, M. R. “The significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories”, *International Journal of Engineering and Technology,* 7(2.29), 737-741, 2018.

[42] Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). “Determinants of early conformance with information security policies”, *Information & Management,* 54(7), 887–901.

[43] Torten, R., Reaiche, C., & Boyle, S. “The impact of security awareness on information technology professionals’ behavior”, *Computers Security,* 79, 68-79, 2018.

[44] Lowry, P. B., Moody, G. D., & Chatterjee, S. “Using IT design to prevent cyber bullying”, *Journal of Management Information Systems,* 34(3), 863-901, 2017.

[45] Menard, P., Bott, G. J., & Crossler, R. E. “User motivations in protecting information security: Protection motivation theory versus self- determination theory”, *Journal of Management Information Systems,* 34(4), 1203-1230, 2017.

[46] Pham, H., Brennan, L., & Richardson, J., "Review of behavioural theories in security compliance and research challenge," In *Informing Science and Information Technology Education Conf.,* Vietnam, 2017, vol. 31, pp. 65-76, Santa Rosa, CA: Informing Science Institute,doi:10.28945/3722.

[47] Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. “The role of cybersecurity and policy awareness in shifting user compliance attitudes: Building supply chain capabilities”, *International Journal of Information Management,* 66, 102520, 2022.

[48] Hong, Y., & Furnell, S. “Motivating information security policy compliance: Insights from perceived organizational formalization”, *Journal of Computer Information Systems,* 62(1), 19-28, 2022.

[49] Ntwari, R., Habinka, A. E., & Kaggwa, F. “Enhancing Bring Your Own Device Security in Education”, *Journal of Science & Technology,* 2(4), 1–18, 2021.

[50] Alanazi, T., Anbar, M., Ebad, S., Karuppayah, S., & Al-Ani, H. A. “Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector”, *Symmetry,* 12(9), 1544, 2020. https://doi.org/10.3390/sym12091544

[51] Farooq, A., Ndiege, J. R. A., & Isoaho, J. “Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior”, *2019 IEEE AFRICON,* 1–8. 4, 2019.

[52] Chen, X., Wu, D., Chen, L., & Teng, J. K. “Sanction severity and employees’ information security policy compliance: Investigating mediating, moderating, and control variables”, *Information Management,* 55(8), 1049- 1060, 2018.

[53] Wangòndu, H., & Munyoki, J., “Effect of Institutional Pressure on BYOD Information Security Policy Compliance: A Case of Two Private and Two Public Kenyan Universities", Ph.D. dissertation, Faculty .S.T, Nairobi Univ., Kenya, 2020.

[54] Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. “Variables influencing information security policy compliance: A systematic re- view of quantitative studies”, *Information Management Computer Security,* 22(1), 42-75, 2014.

[55] Chen, Y., Xia, W., & Cousins, K. “Voluntary and instrumental information security policy compliance: An integrated view of prosocial motivation, self-regulation, and deterrence”, *Computers & Security,* 113, 102568, 2022.

[56] Wang, X., & Xu, J. “Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry?”, *Tourism Management,* 84, 104282, 2021.

[57] Kim, B., Lee, D. Y., & Kim, B. “Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks”, *Behaviour & Information Technology,* 39(11), 1156–1175, 2020.

[58] Vance, A., Siponen, M. T., & Straub, D. W. “Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures”, *Information Management,* 57(4), 103212, 2020.

[59] Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. “Deterrence and prevention-based model to mitigate information security insider threats in organisations”, *Future Generation Computer Systems,* 97, 587-597, 2019.

[60] Tran, D. van, Nguyen, P. v., Le, L. P., & Nguyen, S. T. N. “From awareness to behaviour: understanding cybersecurity compliance in Vietnam”, *International Journal of Organizational Analysis,* 33(1), 209–229, 2025.

[61] Alshare, K. A., Lane, P. L., & Lane, M. R. “Information security policy compliance: A higher education case study”, *Information Computer Security,* 26(1), 91-108, 2018.

[62] Son, J. Y. “Out of fear or desire? Toward a better understanding of users’ motivation to follow IS security policies”, *Information Management,* 48(7), 296-302, 2011.

[63] Johnson, Emmanuel Laggah. "Factors influencing undergraduate students’ intention to adopt information security policies: a correlational study", Ph.D. dissertation, Dept. ITDS, Capella Univ. , USA, 2018.

[64] Zhiling Tu, C., Adkins, J., Yu Zhao, G., Zhiling, C., & Yu, G. “Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory”, *Journal of the Midwest Association for Information Systems,* 2019(1), 11-27, 2019.

[65] Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. “Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory”, *Computers & Security,* 149, 104204, 2025.

[66] Strahle, M. I., “A Quantitative Survey Research Study Examining Predictors of Employees’ Intentions to Accept Predictive Analytics for Insider Threat Monitoring”, Capitol Technology Univ, Washington D.C., USA, 2022.

[67] Hanus, Bartlomiej T. “The Impact of Information Security Awareness on Compliance with Information Security Policies: A Phishing Perspective”, Ph.D. dissertation, Dept. ITDS, North Texas Univ., Denton, Texas, USA, 2014.

[68] Saima Nisar, “The Hybrid Model for Intention to Adopt BYOD From the Perspective of Pakistani Doctors”, Ph.D. Thesis, Coll. Cybersecurity, Utara Malaysia Univ., KL, Malaysia, 2021.

[69] Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. “Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals”. *Computers in Human Behavior,* 68, 190–209, 2017.

[70] Livson, M., Ulanova, K. L., Pertsev, V. V., Dudynov, S. V., & Novikov, A. V. "The Influence of BYOD on Results of Students' Learning", *Propósitos y representaciones*, 9(2), p.49, 2021.

[71] Cox, J. “Information systems user security: A structured model of the knowing–doing gap”, *Computers in Human Behavior,* 28(5), 1849-1858, 2012.

[72] S. Aurigemma and R. Panko, "A Composite Framework for Behavioral Compliance with Information Security Policies," *45th Hawaii Int. Conf. on System Sciences*, Maui, HI, USA, 2012, pp. 3248-3257, doi: 10.1109/HICSS.2012.49.

[73] Herath, T., & Rao, H. R. “Protection motivation and deterrence: A model for security policy compliance in organizations”, *European Journal of Information Systems,* 18(2), 106-125, 2009.

[74] Lian, J. W. “Understanding cloud-based BYOD information security protection behavior in smart business: In perspective of perceived value”, *Enterprise Information Systems,* 15(9), 1216-1237, 2021.

[75] Doargajudhur, M. S., & Dell, P. “The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation”, *Journal of Computer Information Systems,* 60(6), 518–529, 2020.

[76] Wall, J. D., Palvia, P., & D’Arcy, J. “Theorizing the Behavioral Effects of Control Complementarity in Security Control Portfolios”, *Information Systems Frontiers,* 24(2), 637–658, 2022.

[77] Williams, A. S., Maharaj, M. S., & Ojo, A. I. “User behavioral factors and information security standard compliance in Nigerian banks”, International Journal of Computing and Digital Systems, 8(04), 387-396, 2019.

[78] Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. “BYOD security issues: a systematic literature review”, *Information Security Journal: A Global Perspective,* 31(3), 253–273, 2022.

[79] Zeaman, K. D. “Senior Decision Makers’ Behavioral Response to Bring Your Own Device (BYOD) Programs”, Ph.D. dissertation, Coll. B. Tech. & A, Capella Univ., Minnesota, USA, 2025.

[80] Awang, N., Salleh, N. S., Zulkipli, N. H. N., & Zakaria, O. “Optimizing Security Compliance in Bring Your Own Device (BYOD) Through a Hybrid Approach”, *Advances in Computer Science Research,* pp. 498–508, 2024.

[81] Jensen, B. “Motivational Factors in Potential Employees to Accept Restrictive BYOD ISSP in the Workplace”, *Northcentral University ProQuest Dissertations & Theses,* 2018. 10827128, 2018.

[82] Grimes, J., & Marquardson, J. “Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions”, *Decision Support Systems,* 119, 23-34, 2019.

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

[84] A. F. Zahra and R. G. Utomo. "Factors Influencing Student Compliance With University Information Security Policies in Indonesia Using the Unified Model Information Security Policy Compliance (UM-

ISPC)," *Int. Conf. on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia, 2024, pp. 89-94, doi: 10.1109/ICITSI65188.2024.10929144.

[85] Grabowski, M., Pająk, R., & Sagan, A., "Information Security Success Perception: The Role of Response Cost", In *European, Mediterranean, and Middle Eastern Conf. on Information Systems*, 2024, pp. 382-396. Cham: Springer Nature Switzerland, doi:10.1007/978-3-031-81322-1_26.

[86] Siponen, M., Pahnila, S., & Mahmood, M. A. "Compliance with information security policies: An empirical investigation", *Computer,* 43(2), 64-71, 2010.

[87] Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. "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, 2014.

[88] White, J. K., Lucarelli, C., Swain, M., Member, C., Chapman, B., & Capron, R. "Impact of Protection Motivation Theory and General Deterrence Theory on The Behavioral Intention to Implement and Misuse Active Cyber Defense", Ph.D. dissertation, Coll. B. Tech. & A. , Capella Univ., Minnesota, USA, 2017.

[89] Johnston, Z. A., & Mckibbin, W. J. "Exploring Privacy Concern Effect on Organizational BYOD Policies and Security Measures Compliancy", Ph.D. dissertation, Coll. B. & Tech., Capella Univ., Minnesota, USA, 2022.

[90] Meesala, Mohan Kumar. "Security Policy Compliance Among Remote Workers Using BYOD Policies.", Ph.D. dissertation, Faculty. Graduate, Cumberlands Univ., Williamsburg, KY, USA, 2024.

[91] Akande, A. O. "Policy awareness, enforcement, and maintenance: a comparative quantitative approach to information security effectiveness in a Bring Your Own Device (BYOD) environment", Ph.D. dissertation, Coll. B. & Tech., Capella Univ., Minnesota, USA, 2019.

[92] Chen, H., Li, Y., Chen, L., & Yin, J. "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue", *Journal of Enterprise Information Management,* 34(3), 770–792, 2021.

[93] Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. "Keeping customers' data secure: A cross-cultural study of cyber-security compliance among the Gen-Mobile workforce", *Computers in Human Behavior,* 114, 106531, 2021.

[94] Karlsson, F., Karlsson, M., & Åström, J. "Measuring users' compliance: The importance of value pluralism", *Information Computer Security,* 25(3), 279-299, 2017.

[95] Sommestad, T., Karlzén, H., & Hallberg, J. "The Theory of Planned Behavior and Information Security Policy Compliance", *Journal of Computer Information Systems,* 59(4), 344–353, 2019.

[96] Alshammari, M. M. "Understanding the factors that influence university students' behavior toward information security policies", *Management & Sustainability: An Arab Review,*1-20, 2025.

[97] Sarstedt, M., Hair, J. F., Pick, M., Liengaard, B. D., Radomir, L., & Ringle, C. M. "Progress in partial least squares structural equation modeling use in marketing research in the last decade". *Psychology & Marketing*, *39*(5), 1035-1064, 2022.

[98] Nguyen, Hai Vu. "Cybersecurity strategies for universities with bring your own device programs." Ph.D. dissertation, Coll. Mgmt. & Tech., Walden Univ., Minnesota, USA, 2019.

[99] Al-Shanfari, I., Yassin, W., & Abdullah, R. "Identify the factors affecting information security awareness and weight analysis process", *International Journal of Engineering and Advanced Technology (IJEAT),* 9(3), 534542, 2020.

[100] Doe, J., & Roe, S. "Perceptions of BYOD sanctions: A comparative study among university students", *Journal of Cybersecurity Education,* 10(2), 123-138, 2019.

[101] Brown, D. A. . "Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies", Ph.D. dissertation, Coll. Mgmt. & Tech., Walden Univ., Minnesota, USA, 2017.

[102] Tsohou, A., Karyda, M., & Kokolakis, S. “Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs”, *Computers Security,* 52, 128-141, 2015.

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

[104] Lu, Y., Karunasena, G., & Liu, C. “Exploring beyond-compliance behaviors of Australian building practitioners: A cluster analysis”, *Energy Research & Social Science,* 121, 103969, 2025.

[105] Kholoanyane, M. E. “Security awareness and training policy guide- lines to minimise the risk of BYOD in a South African SME”, *Doctoral dissertation, North-West University (South Africa),* 2020.

[106] I. M. Al-Harthy, F. A. Rahim, N. Ali and A. P. Singun, "Theoretical Bases of Identifying Determinants of Protection Intentions towards Bring - Your-Own-Device (BYOD) Protection Behaviors," *2019 First Int. Conf. of Intelligent Computing and Engineering (ICOICE)*, Hadhramout, Yemen, 2019, pp. 1-9, doi: 10.1109/ICOICE48418.2019.9035139.

[107] Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. “A dimension- based information security culture model and its relationship with users’ security behavior: A case study in Malaysian higher educational institutions”, *Information Security Journal: A Global Perspective,* 28(3), 55-80, 2019.

[108] Stewart, H., & Jurjens, J. “Information security management and the human aspect in organizations”. *Information Computer Security,* 25(5), 494-534, 2017.

[109] Al-Omari, A., El-Gayar, O., & Deokar, A. “Information security policy compliance: The role of information security awareness”, *International Journal of Information Management,* 32(4), 360-367, 2012.

[110] Ifinedo, P. “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory”, *Computers & Security,* 31(1), 83-95, 2012.

[111] Thompson, N., McGill, T. J., & Wang, X. “Security begins at home: Determinants of home computer and mobile device security behavior”, *Computers Security,* 70, 376-391, 2017.

[112] Balagopal, N., & Mathew, S. K. “Exploring the factors influencing information security policy compliance and violations: A systematic literature review”, *Computers & Security,* 104062, 2024.

[113] Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes- Sebastián, M. G. “Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity”, *Future Business Journal,* 11(1), 28, 2025.

Appendix A

Table 3: Questionnaire Items

Key factors	Items	The relationship criteria
Perceived Threat Severity	PTS.1	I have experienced that the loss of data is a severe problem for my organization due to hacking. [111]
	PTS.2	I believe security incidents threaten an organization's and its users' productivity and profitability. [73]
	PTS.3	I have experienced incidences where people accessed confidential information without my consent/knowledge. *
Perceived Threat Vulnerability	PTV.1	I could fall victim to a malicious attack if I fail to comply with my organization's information security policy. [110]
	PTV.2	Losing personal data to a malicious attack is a grave issue. [111] *
	PTV.3	I believe that must protect my organization's information will reduce illegal access to it. *
Security Self-Efficacy	SE.1	I would be able to follow the information security policies even if there was no one around to help me. [109]
	SE.2	I could do proactive security to protect the organization's data easily while using personal devices for work purposes. [111]
	SE.3	I would feel comfortable following the information security policies on my own. [109]
Perceived Response Efficacy	RE.1	Threats to my organization's data can be reduced by complying with the information security policies of using my devices. [73] *
	RE.2	Enabling the information security policies of using my devices will provide more protection and security against hackers stealing sensitive data. [110], [111] *
	RE.3	If I follow the organization's information security policies, I can make a difference in helping to secure my organization. [73]*
Attitude	ATT.1	I believe adopting information security policies is very important for my organization [73]
	ATT.2	I feel that compliance with Information Security Policies is reasonable. [110], [37]
	ATT.3	I believe adopting information security policies is beneficial. [73]
Subjective Norms	SN.1	My colleagues think that I should comply with information security policies when using my devices. [73] *
	SN.2	My managers think that I should comply with all BYOD policies. [109] *
	SN.3	To my knowledge, most users comply with the organization's information security policies. [73] *
Perceived Behavioral Control	PBC.1	I have the necessary skills and competencies to fulfil the requirements of the information security policies. [73] *
	PBC.2	I can easily monitor my devices when they hang up. (developed) *
	PBC.3	I have sufficient knowledge and skill to keep my organization's data safe while sharing it using my devices. *
Perceived Severity of Sanctions	PSS.1	A user who breaks information security policies for the first time could get punishment. [73]
	PSS.2	I deserve punishment if I violate the confidentiality of organizational information. [99]
	PSS.3	If I were caught intentionally violating security policy, I think the punishment would be very severe. [73] *
Perceived Certainty of Sanctions	PCS.1	If I violated security policy, the probability I would be caught. [73] *
	PCS.2	If I do not comply with information security policies, I will receive a personal reprimand in oral or written assessment reports. *
	PCS.3	The likelihood that the organization would discover that I installed malicious or pirated software is very high. *
Awareness of ISP compliance	ISA.1	I have sufficient knowledge of the information security policies in my organization. [1] *
	ISA.2	I have received education about information security threats and their negative consequences. [82] *
	ISA.3	I am using Passwords or fingerprints on my devices at work. (developed)
	ISA.4	In my organization, users are briefed on the consequences of modifying BYOD data in an unauthorized way, [1]
	ISA.5	I understand the risk of information security incidents when using my devices. (developed)*
Behavioral Intention	BI.1	I am sure I would comply with the information security policies to protect information resources on my devices at the workplace. [103] *
	BI.2	I intend to report all information about security incidents to others to reduce the risk and increase awareness. [109] *
	BI.3	I would use approved applications and software based on information security policies admitted by the management. (developed)*

* Developed by expert's comments based on (author)

Appendix B

Appendix B. the statistics of academic staff and students in public universities for 2020-2021

Bilangan Staf Akademik mengikut Taraf Warganegara dan Jantina berdasarkan Universiti Awam (UA), 2020-2021

Number of Academic Staffs by Citizenship and Gender in Public Universities 2020-2021

Jadual *Table* **2.9**

Bil. *No.*	UA *Public Universities*	Tahun *Year*	Warganegara / *Malaysian*			Bukan Warganegara / *Non-Malaysian*			Jumlah / *Total*		
			L / *M*	P / *F*	J / *T*	L / *M*	P / *F*	J / *T*	L / *M*	P / *F*	J / *T*
1	UM	2021	805	1,086	1,891	137	60	197	942	1,146	2,088
		2020	786	1,053	1,839	145	61	206	931	1,114	2,045
2	USM	2021	879	1,093	1,972	52	12	64	931	1,105	2,036
		2020	899	1,098	1,997	54	13	67	953	1,111	2,064
3	UKM	2021	846	1,136	1,982	49	10	59	895	1,146	2,041
		2020	876	1,148	2,024	58	12	70	934	1,160	2,094
4	UPM	2021	747	1,052	1,799	26	5	31	773	1,057	1,830
		2020	750	1,056	1,806	27	4	31	777	1,060	1,837
5	UTM	2021	835	772	1,607	43	11	54	878	783	1,661
		2020	865	755	1,620	62	15	77	927	770	1,697

Data sehingga 30 November 2021 / *Data as of 30 November 2021*

Bilangan Enrolmen Pelajar mengikut Taraf Warganegara dan Jantina berdasarkan Universiti Awam (UA), 2020-2021

Number of Students' Enrolment by Citizenship and Gender in Public Universities 2020-2021

Jadual *Table* **2.3**

Bil. *No.*	UA *Public Universities*	Tahun *Year*	Enrolmen / *Enrolment*						
			Warganegara / *Malaysian*			Bukan Warganegara / *Non-Malaysian*			Jumlah / *Total*
			L / *M*	P / *F*	J / *T*	L / *M*	P / *F*	J / *T*	
1	UM	2021	12,019	19,440	31,459	2,553	2,460	5,013	36,472
		2020	11,927	19,845	31,772	2,266	1,847	4,113	35,885
2	USM	2021	10,656	17,898	28,554	2,793	2,494	5,287	33,841
		2020	10,629	17,994	28,623	1,922	1,129	3,051	31,674
3	UKM	2021	9,525	18,377	27,902	1,637	1,235	2,872	30,774
		2020	10,068	18,734	28,802	1,320	722	2,042	30,844
4	UPM	2021	7,635	15,727	23,362	2,833	2,928	5,761	29,123
		2020	7,710	15,993	23,703	2,687	2,197	4,884	28,587
5	UTM	2021	14,037	13,275	27,312	3,555	1,412	4,967	32,279
		2020	14,539	13,703	28,242	3,489	1,169	4,658	32,900

Data sehingga 30 November 2021 / *Data as of 30 November 2021*