Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETERMINANTS OF BYOD PROTECTION BEHAVIOR: AN EMPLOYEE'S PERSPECTIVE

IBRAHIM MOHAMMED AL-HARTHY[1,*], NOR'ASHIKIN ALI[2]

[1]College of Computing & Informatics, Universiti Tenaga Nasional, Malaysia
[2]College of Graduate Studies, Universiti Tenaga Nasional, Malaysia
[*] Email: Ibrahim.alharthy@hct.edu.om

ABSTRACT

Bring Your Own Device (BYOD) allows employees to access the organizational network via their devices/technology. This trend is beneficial to the employees in terms of greater flexibility, apart from productivity and cost savings for the company. Enabling employees to use their own devices at the workplace may lead the company to become vulnerable to information security threats as employees do not possess the right understanding of protecting their devices. This study analyzed the factors that determine employees' behavioral intention and their actual protection behavior in protecting their devices in BYOD environment. A self-administered questionnaire was conducted with 383 government employees in Oman. The results indicated that perceived vulnerability, perceived severity, response cost, subjective norm, perceived behavioral control, and knowledge influenced employees' BYOD intention protection behavior while perceived vulnerability, perceived severity, response efficacy, response cost, attitude, subjective norm, and perceived behavioral control were found to influence BYOD protection behavior. Contrarily, response efficacy, security self-efficacy, attitude, and information security awareness were found to be nonsignificant on protection intention. The findings also revealed that the mediator (protection intention) has a considerable beneficial impact on the dependent variable (protection behavior). Hence, employers should develop an all-encompassing approach to improve their employees' BYOD usage protection behavior to secure the organization's assets.

Keywords: *BYOD, Protection Behavior, Protection Intention, Survey, Structural Equation Modelling*

1. INTRODUCTION

Since the use of smartphones and tablets has become more prevalent in the workplace, Bring Your Own Devices (BYOD) has become a new trend among organizations. Mobile phones, smart phones, laptops, and tablets are widely used in the BYOD trend as it provides employees more flexibility to complete their tasks remotely without having to be physically present at offices. BYOD co-existed with IT consumerization where the devices were incorporated into business and government usage from personal use [1]. In a BYOD environment, employees use their devices to access their organizations' networks and data for work-related purposes [2]. They no longer have to carry multiple devices for work and personal use, and they no longer have to learn to operate various makes and models of devices. BYOD trend is becoming more prevalent since the emergence of Covid-19 where governments and corporates worldwide opted to switch to an alternate method of working, work from home [3]. Movement restrictions and social distancing regulations drove organizations to adopt BYOD to continue employee engagement at work without disruption. According to the global market ideas, BYOD stock was anticipated to be worth more than $300 billion by 2020 [4].

Although surveys indicated that bringing your device to work improves employee job performance and productivity, improves communication between employees [5], and saves operational cost [3], the use of personal devices at work poses a greater threat than in a traditional IT setting. They are not only at risk of losing or misplacing their devices, but they may also use apps or infected links that could make their devices vulnerable to hackers and cyber

security threats such as malicious insiders and malware attacks [6, 7, 8, 9]. Hence, such vulnerabilities increase the likelihood of data loss [10]. Also, with staff working from home during the pandemic, there is insufficient organizational power over individual personal devices and inadequate access control [11], leading to security concerns in businesses. Furthermore, the lack of employee awareness in protecting their devices ([12, 13, 14, 15] exacerbated the hazards associated with employees' lack of knowledge of personal device security settings [16, 17, 18]. According to a poll conducted by Kaspersky Lab, 52% of users do not password-protect their mobile devices, while only 22% utilize anti-theft software [19].

Over the last decade, several studies focused on information security behavior ([20, 21, 22, 23]. However, BYOD security research is still in its infancy [24], with limited research on information security behavior associated with home and personal use of information systems [25]. According to [25], one of the largest difficulties in cybersecurity is employee security awareness. Employees' security behavior in managing and securing their devices is crucial in an organization's BYOD strategy [26, 27, 28]. It is impossible to improve the performance of information security policies in enterprises without employees' initiatives and knowledge to secure their organizations' IT resources (e.g., software, hardware, and data) [29]. Therefore, businesses must recognize the necessity of safeguarding their assets by ensuring that BYOD is used safely. Apart from instilling technical measures to ensure BYOD security, non-technical measures should also be considered. Developing an effective policy without understanding the elements influencing employees' BYOD protection behavior can be difficult.

2. LITERATURE REVIEW

This study seeks to investigate the determinants of employees' protection intention and their protection behavior in using their devices in a BYOD environment. This study is organized as follows. Firstly, the overview of BYOD, BYOD risks, and underlying theories used for building the structural model, and hypotheses development based on PMT and TPB theories were reviewed, followed by research methods and the results of the structural model. The discussion section revealed the key findings and described the theoretical and practical implications, limitations, and future work. The final section concluded the results.

2.1 BYOD

BYOD refers to the exercise where individuals in an organization or institution use their equipment or gadgets to complete their work. [30] stated that smartphone users are constantly increasing every year and is becoming the dominant device to access internet resources. In 2021, the number of smartphone users globally was projected to be approximately 6.3 billion [31] and it was estimated that 5.22 billion users use mobile devices for work-related tasks. Nearly 87% of organizations rely on their employees to use their personal devices for work-related tasks [32], describing the current trend of BYOD. The BYOD strategy is considered a bottom-up approach, where users employ and get accustomed to new technologies before using them at their workplace whereas traditionally, employers deploy new technologies for the employees to use. The BYOD includes the following devices: laptop computers, netbook computers, smartphones/handhelds, tablet computers, e-book readers, and audio players [33]. The survey by [34], indicated that personal computers were the most common device (96.7%) used in work, followed by smartphones (66.0%). Smartphones are becoming increasingly popular as work devices, with two-thirds of the respondents reported using a smartphone for work.

During the COVID-19 pandemic, many employers failed to consider the potential security threats that caused mass disruption around the world as employees were required to work from home, where they were required to enter systems through private devices [35]. One additional risk of data loss through BYOD usage when employees working from home during a pandemic like COVID-19 is that in the organization, employees may be using secure

internal computer systems and updated computers, but at home, the same employees could be using insecure or outdated devices that are more vulnerable to attack [36]. The lack of employees security when using BYOD to accomplish work remains a major challenge for organizations [37]. It's the context case of employees' use of BYOD as those devices have been used mainly for their own but also to accomplish work [38, 39]. The implementation of BYOD makes it difficult for organizations to control their data which are being accessed by their employees using personal devices. Although some organizations initiated BYOD policies, the policies are generic and do not account for other different types of devices, OS and mobile software that employees use in a workplace [40].

2.2 Risks of BYOD

Despite the advantages of BYOD application, this policy is prone to cyberattacks. The issues resolved around BYOD are primarily on information safety and privacy [41]. Moreover, severe risks arise with getting your phone into the office and the secured network. According to [42], the types of BYOD hazards include robbery or robbed computer, access to customer details such as username and password, integrated records, private financial data, internet addresses, and email addresses.

Various risks and problems associated with the implementation of BYOD among employees include data loss and data breaches that could incur a huge financial loss and cost the organization its reputation [43]. One in five organizations (21%) suffer security breaches involving mobile devices due to malicious Wi-Fi hotspots connections and malware [44]. [45] indicated that many organizations are still running a BYOD without applying a BYOD policy or with BYOD policies only applicable to a specific group of employees and devices. This practice could lead to a loss of confidential data if an employee's device is stolen or goes missing. For instance, the employee might be saving their passwords (personal and that of the organization) in unsecured note applications, which would be easy for hackers to access once they have breached the organization's account [46].

Organizations need to understand the vulnerabilities and security risks introduced when BYOD is implemented, apart from the legal issues which may arise through disgruntled employees. Generally, many companies ignore or do not realize the possibilities of such legal implications when they readily adopt BYOD. The organizations are more focused on perceived savings through the adoption of BYOD, which overshadows the loss of valuable information or lawsuit due to privacy infringement when personal and organization data are jeopardized. Even though companies adopt BYOD solutions to separate organization and personal data, privacy regulations need to be considered for data such as text messages and photo galleries [47].

2.3 Protection Motivation Theory (PMT) And Theory of Planned Behavior (TPB)

Protection Motivation Theory (PMT) is considered powerful in explaining and predicting people's protection attitudes and behaviors [48], and has been validated as a suitable model for understanding security behavior [49]. PMT has been deployed in information system security research to understand individual's intentions and protection behaviors [50, 51, 26, 27, 52]. Most of the previous studies of behavioral IS security focused on intentions. For example, PMT explained employees' protection intentions and behaviors based on adopting antivirus protection applications [53], performance of devices-protection operations [54], and security policies compliance [51, 55]. There is still a lack of explicit inclusion of actual protection usage [56]. This research, therefore, focuses on the actual usage of BYOD protection behavior via BYOD protection intention.

In this study, PMT posits that an individual's protective behavior is based on two concepts namely threat appraisal and coping appraisal. In short, the response towards a risk faced by and individual is influenced by threat and coping appraisals [57, 58]. Threat appraisals depict the level of threat felt by an individual. It is based on: (1) how severe the threats would be to an individual (perceived severity); and (2) how vulnerable an individual is to be exposed to the threats (perceived vulnerability) [48, 50]. Meanwhile, coping appraisal refers to the evaluation of one coping and adapting with the

threats, which encompasses three components: 1) how effective the coping response is in reducing or eliminating the threat (response efficacy); 2) whether one can perform coping response (self-efficacy); and 3) one's coping responses with inconveniences incurred such as monetary, time, and efforts [59, 48]. Essentially, the protection motivation increases when threat appraisals are combined with coping appraisals leading to a more adaptive behavior among individuals.

PMT and TPB were never integrated as one conceptual model to study employees' security behavior towards BYOD. According to [23] and [24], future studies should focus on factors that can significantly affect BYOD protection behavior when developing models for employees who use personal devices at work. Consequently, the present study focuses on five constructs (adopted from PMT) in security behavior when using BYOD: (1) perceived vulnerability; (2) perceived severity; (3) response efficacy; (4) self-efficacy; and (5) response cost. These five antecedents of protection intention lead to protection behavior when using BYOD [60, 61, 62, 63, 64, 65, 66, 67, 68, 23, 69]. Although PMT has been used in many behavioral IS securities studies, [24] suggested that PMT requires extension and integration with other theories in future studies to increase its explanatory power.

3. HYPOTHESES DEVELOPMENT

Based on the arguments highlighted above, the proposed model as depicted in Fig 1 combined PMT with TPB, a predominant theory that has been applied in information security research involving social behavioral theories in the extant literature [70] and included other additional factors: security awareness and knowledge. The 10 factors that were included in the research model were perceived vulnerability, perceived severity, response efficacy, response cost, attitude, subjective norm, perceived behavioral control, security self-efficacy, information security awareness, and knowledge. The mediating variable is protection intention, while the outcome variable is protection behavior.

3.1. Perceived Vulnerability (PV)

PV is a construct in PMT [71, 72]. PV is defined as a person's assessment of their likelihood of being confronted with a threat [55]. Previous studies revealed that employees' behavioral intention towards smartphone-security compliance was influenced by perceived risk vulnerability [69]. In another study, [73] investigated the link between PV and response costs in terms of information security behavioral intention. The authors discovered that information security behavior was nonsignificantly affected by the vulnerability to online information security occurrences. In essence, individuals choose protective behaviors if they perceive their vulnerability to perceived threats. For instance, if users believe that their passwords may be hacked, then they are more likely to take protective measures. Thus, we hypothesized that:

H1a: *Perceived vulnerability has a positive influence on BYOD usage protection intention.*

H1b: *Perceived vulnerability has a positive influence on BYOD usage protection behavior.*

3.2 Perceived Severity (PS)

PS refers to people's perception on the outcomes of threat protection when using their devices and their view on the harmful consequences of non-compliance with protective behaviors [48]. The author identified that PS had a significant effect on behavioral intention towards smartphone safety behavior among female employees than male employees. Moreover, a study by [73] hypothesized that perceived severity of online information security has a harmful association with the information security problem behavior of teachers. In this study, PS is associated with the employee's assessment of the seriousness of a security threat and its associated consequences. If an employee perceives a security threat to the organization's resources to be severe, he or she is more likely to engage in security measures such as protection behavior of BYOD. Conversely, when the perceived severity of the risks has diminished, the employees will bring down their guard. Hence, we hypothesized that:

H2a: *Perceived severity has a positive influence on BYOD usage protection intention.*

H2b: *Perceived severity has a positive influence on BYOD usage protection behavior.*

3.3. Response Efficacy (RE)

RE which is part of PMT is a coping appraisal factor, where it received less attention in research compared to the other factors. RE is defined as the right and efficient response or protective behavior in the face of a threat, risk, or vulnerability to privacy loss [74, 75]. According to [76], high perceived response efficacy encouraged employees' to follow BYOD applicable policies. Additionally, RE was determined to be the most consistent predictor among the reported PMT factors compared to the multicollinearity risk and management assessments [77]. It was specifically posited in PMT that a person intention to adopt the behaviors increases based on the perceived efficacy of the behaviors [48]. We hypothesized that:

H3a: *Response efficacy has a positive influence on BYOD usage protection intention.*

H3b: *Response efficacy has a positive influence on BYOD usage protection behavior.*

3.4. Response Cost (RC)

RC refers to the employee's cost of engaging in a given protective behavior [48]. RC does not only include monetary expenses but also time, effort or inconvenience that may be associated with the protective behavior. Hence, it is posited that when perceived response cost is high, individuals will be less inclined to engage in protective behavior. Conversely, the behavior may be adopted if it only incurs a small cost. This view was also supported by [65], who discovered a substantial negative link between response cost and the propensity to adopt security behavior among smartphone users. Therefore, we hypothesized that:

H4a: *Response cost has a negative influence on BYOD usage protection intention.*

H4b: *Response cost has a negative influence on BYOD usage protection behavior.*

3.5. Security Self Efficacy (SSE)

One of the other components of PMT is SSE variable. Previous PMT studies revealed that SSE is accepted as a precursor to protective behavior. [78] anticipated that individuals with high esteem for their self-efficacy are less fearful of the perceived risks than those with low regard for their abilities to deal with such security issues. Other studies have also indicated that self-efficacy can significantly and positively influence information security intentions. For example, [79] stated that when a person believes that he or she is capable of performing a coping behavior to prevent the loss and theft of mobile devices, they are influenced to engage in coping action. Meanwhile, [61] documented that BYOD users' perceptions of self-efficacy can positively impact their intention to subscribe to anti-malware software. Similarly, this study also aims to confirm that an employee's protection intention and behavior may increase if they believe that they can comply with BYOD policies. Nonetheless, this study adopts the security self-efficacy that refers to the insiders' protective roles and associated behaviors with which they must engage to protect organizational information [52]. For individuals to adopt good protective behavior, they are expected to believe in their protective roles to protect their devices. Thus, we include SSE as a determinant of protection intention and behavior to hypothesize that:

H5a: *Security self-efficacy has a positive influence on BYOD usage protection intention.*

H5b: *Security self-efficacy has a positive influence on BYOD usage protection behavior.*

3.6. Attitude (ATT)

ATT is defined as a person's overall evaluation of performing the actual behavior. An individual's positive or negative attitude towards engaging in a particular behavior is referred to as attitude [80, 60]. The influences on social network users' behavior (attitude) include gender, age, and career [81]. Meanwhile, [82] established an Information Security Culture (ISC) model to improve effectively employees' protection behavior in an organization with seven newly formulated characteristics to investigate its impact on workers' Information Security Policy (ISP) compliance behavior, which includes attitude. They anticipated that ISC can influence employees' attitudes regarding ISP compliance, whereas their intention to comply with ISP is influenced by their attitude towards ISP compliance. Similar to TPB's theory, this study is in view that individuals with a positive attitude towards protecting their devices will have favorable tendencies to comply with BYOD

protection policies. Thus, we hypothesized that:
H6a: *Attitude has a positive influence on BYOD usage protection intention.*
H6b: *Attitude has a positive influence on BYOD usage protection behavior.*

3.7. Subjective Norms (SN)

SN refer to the belief that a person or group of people in their surroundings could influence them to engage in a particular behavior [63]. TPB stipulated that powerful figures (such as bosses, co-workers, and parents) could have some control over an individual's behavior by influencing their compliance with a new security policy. [83] monitored the Belgian population for the effects of subjective norms on their behavior intention. They proposed that subjective norm is a useful predictor of protective behavior. According to [84], information security policies can significantly impact the creation of subjective norms on information security behavior within organizations. Moreover, subjective norms can create social pressure on people to perform or refrain from performing a given action. In short, subjective norms have a positive correlation with security intents. Previous studies revealed the link between subjective norms and security intentions [63, 85]. They agreed that employees are more likely to be influenced by their co-workers (i.e. superiors, peers, and subordinates) in their decisions whether to engage in IS security compliance. We, thus, hypothesized that:
H7a: *Subjective norm has a positive influence on BYOD usage protection intention.*
H7b: *Subjective norm has a positive influence on BYOD usage protection behavior.*

3.8. Perceived Behavioral Control (PBC)

PBC refers to a person's perceived ease or difficulty in performing a behavior. A previous study demonstrated a significant and positive effect of PCB on people's intention to receive COVID-19 vaccines [86]. Similarly, PBC had a significantly direct effect on adherence behavior for diabetes [87]. Although PCB has long been tested in health behaviors [88], information on the effects of PCB on security behaviors is limited. Therefore, this study indicated the employee's belief regarding the efficacy needed for BYOD protective behavior. PCB affects BYOD usage protection intention and thus, protection behavior. We hypothesized that:
H8a: *Perceived behavior control has a positive influence on BYOD usage protection intention.*
H8b: *Perceived behavior control has a positive influence on BYOD usage protection behavior.*

3.9. Information Security Awareness (ISA)

ISA is defined as the degree or extent to which all employees understand the importance of information security policies, rules, and regulations, and take responsibility for protecting their organization's information by acting accordingly [89, 90]. [91] divided ISA into two categories namely general information security awareness (GISA) and information security policy awareness (ISPA). ISA plays an important role in reducing the risk of security breaches in organizations. [92] predicted that GISA for workers in the TPB prediction model can improve the intentions to follow information security policies. [67] concluded that management can provide basic in-house information security awareness workshops and training to promote a favorable attitude towards information security concerns among their employees. Thus, we hypothesized that:
H9a: *Information security awareness positively influences BYOD usage protection intention.*
H9b: *Information security awareness positively influences BYOD usage protection behavior.*

3.10. Knowledge (KNOW)

KNOW attribute is based on the knowledge-attitude-behavior (KAB) model [93, 94]. It is defined as a person's understanding and use of information technology, together with their comprehension of the process of protecting company data using their personal devices [95]. Based on the KAB model, an employee's level of knowledge on information security policy, rules, and regulations increases and improves their attitude towards information security behavior [96]. Meanwhile, [97] mentioned that individual KNOW is positively related to information security culture in BYOD usage protection intention. Additionally, [98] indicated that individuals who are aware of information security when using BYOD possess a more positive attitude as they present protection intentions. These studies empirically tested the importance of knowledge in influencing a

person's behavior. Hence, we hypothesized that:
H10a: *Knowledge has a positive influence on BYOD usage protection intention.*
H10b: *Knowledge has a positive influence on BYOD usage protection behavior.*

3.11. Protection Intention (PI)

Several studies concerning security behavioral intentions used TPB as an underlying theory [92, 99]. According to the theory, behavior is determined by the intentions to perform the behavior. However, previous studies focused on intention as the dependent variable, which is determined by other variables. The Protection Motivation Theory (PMT) is a breakthrough explanatory model for anticipating individuals' desire to engage in protective acts [100]. The protection intention is described as a protection motive that motivates, sustains, directs, and activates an individual's intentions to perform the recommended precautionary behavior [101]. PMT was incorporated by [54] and [51] in their studies to investigate individuals' intentions to protect organization resources and data through antivirus applications, general PC-security operations and adhere to their organization's information security policies. [16] demonstrated that the relationship between mobile information protection intention and mobile information protection behavior was positive. We hypothesized that:
H11: *BYOD usage protection intention has a positive influence on BYOD usage protection behavior.*

3.12. Protection Behavior (PB)

The term protection behavior was adapted from PMT [48]. Users are engaged in protection behaviors when they try to secure their organization's data and technical resources from information leaks when using BYOD by installing antivirus, firewalls, updating the OS patches, and being vigilant when opening unknown files [102, 103, 104]. For these preventive measures to be effective, users should be motivated to engage in their protection behaviors. Factors that influence their protective behaviors should be addressed because developing clear information security policies and implementing BYOD-related protection measures are no longer sufficient to address the problem [105]. Since many individuals are unaware of the impending threats of cyber-attacks, it is important to explore ways to engage them in preventive behaviors in response to such potential threats. BYOD usage protection behavior is an actual enactment to implement the protection personal devices settings; the protection behavior is an actual decision that employees could be candid when using BYOD [16].

3.13. Mediating Effect of Protection Intention (PI)

When a third latent determinant is placed between two latent determinants, the mediating effect is formed to act as an intermediary between the two latent determinants [106]. It is important to note that the mediator is not the same as the moderator. In the mediator-predictor connection, the predictor is generally an antecedent of the mediator, where the mediator shifts its roles from effect to causes [107].

Protection intention drives protection behavior and the employees' responses towards a situation [92, 16]. Many studies back this up in the literature, and major theories including TRA [108], TPB [109], DTPB [110] and PMT [110], include it as a mediator toward protective behavior [48]. Furthermore, Fishbein and Ajzen (1975) pointed out that having a purpose to perform a specific protective behavior is a prerequisite.

As a result, many studies have included it in their models in the past, and it is a significant determinant of behavior in a variety of models and frameworks [111, 112, 110, 113, 114, 115]. Previous literature supported and emphasized the importance of the mediating role of protection intention between ATT, SN, PBC and protection behavior [116, 108]. Additionally, other studies have also identified the mediating influence of protection intention between PV, PS, SSE, RE, EC, and protection behavior [48, 102].

Also, protection intention mediates the relationships between information security awareness, knowledge, and protective behaviors [119; 62, 64, 12]. However, there is a lack of research in academia evaluating the mediating effects of protection intention (PI) between the determinants and protection behavior (PB) [121].

In the current study, the protection intention (PI) is evaluated as a mediator between the 10 determinants and protection behaviors (PB) (Figure 1).

The proposed model as depicted in Figure 1, combines two theories, TPB and PMT, and additional variables, information security awareness and knowledge (KNOW). Protection intention is the mediating variable, while protection behavior is the dependent variable (outcome variable).

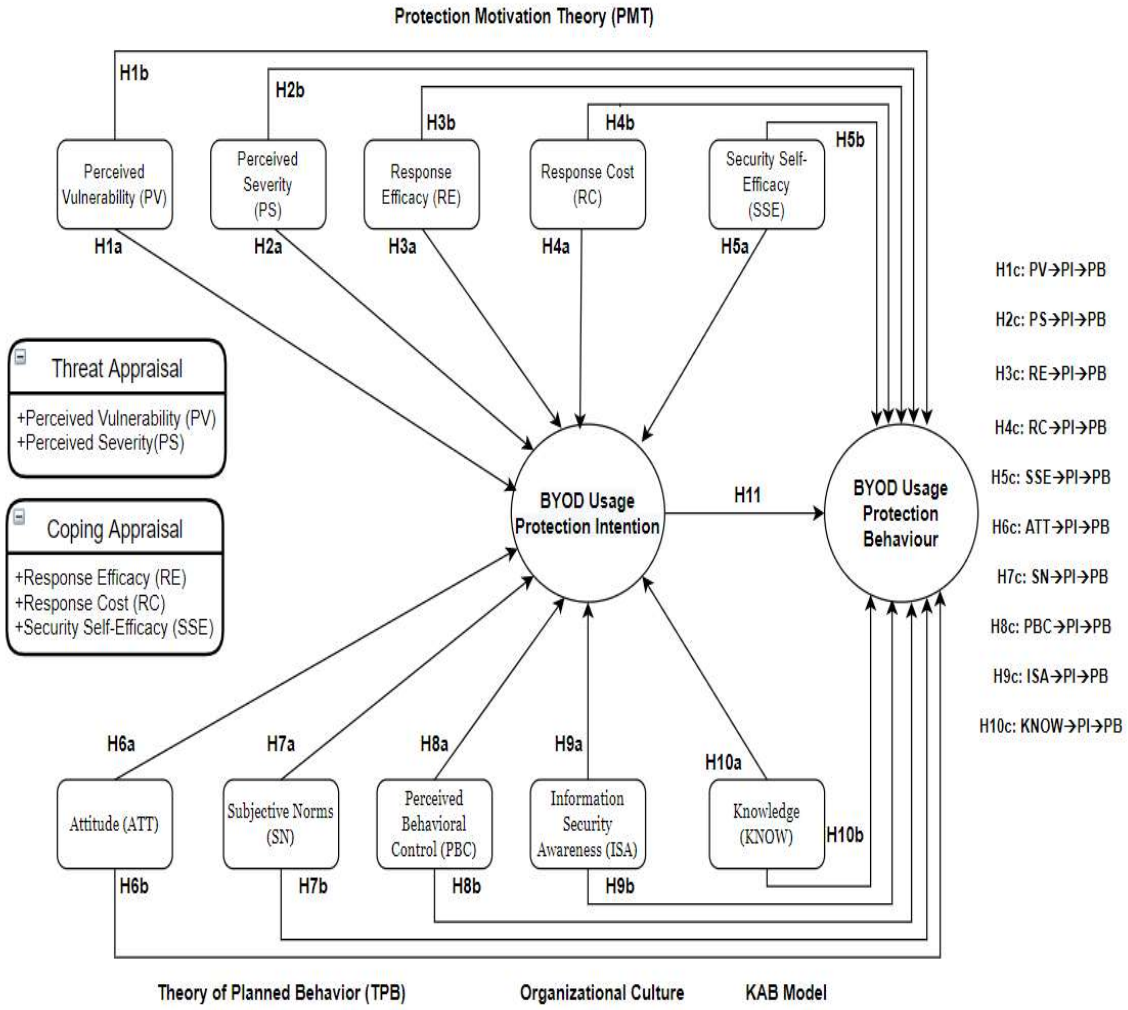

Figure 1: Conceptual Research model

4. RESEARCH METHODOLOGY

4.1. Sampling and Data Collection

A total of 383 self-administered questionnaires were distributed to personnel in the government sector in Oman. The participants of this study comprised public servants (62 government ministries, agencies, and institutions) in Oman who use their personal devices to accomplish their daily tasks [121]. The questionnaire was drafted in English and Arabic languages as these languages are widely used in Oman. According to [123] questionnaire survey is an appropriate approach to test hypotheses. This study employed a structural equation modelling approach (SEM-PLS) to test the relationships among the variables adopted in a conceptual model of the present study.

4.2. Measurements

A survey instrument was used in a quantitative research approach to explore and evaluate the relationships in the postulated model. The items for each of the 12 constructs are presented in Table 1. The items were adopted from well-established and published former works based on the models or theories. Also, the instrument adapted, their construct validity and internal consistency and reliability (i.e., Cronbach's alpha and construct validity based on [138] were tested, validated, and proven its scales. All items were scored using a five-point Likert scale (Likert, 1932), "1 = strongly disagree" to "5 = strongly agree".

4.3. Measurement Model Assessment

According to [132], the outer measurement model used evaluates the factor analysis to which extent the observed variables are loaded on their underlying construct. To evaluate the model, Cronbach's α and composite reliability were checked for the three stages, namely internal reliability, convergent validity, and discriminant validity. Once the three stages were achieved, we proceeded to the structural model analysis (hypotheses testing).

The outer model/Confirmatory Factor Analytic (CFA) is recommended to confirm the underlying relationship between the observed variables and the latent factors [123]. The underlying latent variable explains the items variance that indicates item reliability [124] while the latent construct illustrates the standardized outer loadings (absolute correlation), which must be more than 50% [132]. The composite reliability was higher than the cut-off value of 0.70 [125], while Cronbach's α was higher than the recommended value of 0.7 [126]. The Average Variance Extracted (AVE) for every latent variable was higher than the recommended value of 0.5 (50%), indicating that every construct could explain more than half of the variance to its measuring items on average [127]. The measurement model criteria for model fit are summarized in appendix A.

The discriminant validity results are presented in appendix B. The item loading of one determinant must be higher than its loading on other determinants. The table elucidated that all items load with the highest values to their related constructs, at least 0.1 higher than the cross-loading values. The results indicated that the determinant items assessed the intended construct [136]. The cross-loading of this study method validated the discriminant validity.

5. DATA ANALYSIS AND RESULTS

The route coefficient evaluation result indicated that 14 hypotheses out of 21 were significant. The 14 hypotheses were statistically significant at a p-value < 0.05 with anticipated sign directions. While the route coefficient values (β) ranged between 0.081 to 0.332. According to Figure 2, 14 direct associations (p-values < 0.05 and t-values > 1.96) were found to be significant.

As for the direct relationships between the determinants on the protection intention, the results revealed that H1a (PV -> PI, p = .006), H2a (PS -> PI, p = .000), H4a (RC -> PI, p = .007), H7a (SN -> PI, p = .014), H8a (PBC -> PI, p = .042), and H10a (KNOW -> PI, p = .032) were statistically significant. Meanwhile, H3a (RE -> PI, p = .726), H5a (SSE -> PI, p = .672), H6a (ATT -> PI, p = .593), and H9a (ISA -> PI, p = .032) were statistically insignificant.

While, the direct relationship between the determinants of protection behavior indicated that H1b (PV -> PB, p = .001), H2b (PS -> PB, p = .000), H3b (RE -> PB, p = .033), H4b (RC -> PB, p = .000), H6b (ATT -> PB, p = .016), H7b (SN -> PB, p = .011), and H8b (PBC -> PB, p = .025) were statistically significant.

The remaining hypotheses, H5b (SSE -> PB, p = .685), H9b (ISA -> PB, p = .131), and H10b (KNOW -> PB, p = .457) were statistically insignificant. The direct relationship between the protection intention and the protection behavior, H11 (PI -> PB, p = .000) was statistically significant. Table 1 and Figure 2 summarized the findings.

5.1. Path Coefficient Analyses

The path coefficient of Smart-PLS is similar to the standardized in multiple regression analysis. Since PLS does not require distribution assumptions, the bootstrapping approach was used to estimate the t-statistics and confidence intervals [137]. To observe the relevant relationships in the inner path model, path estimation or hypothetical relations was used.

The regression coefficient (β) was used to investigate every hypothetical path in the framework. The value was tested using the PLS bootstrap technique to determine whether the hypotheses of the structural model were accepted [138, 139, 140]. To account for a specific effect of relationships in the model, the path coefficient value must be at least 0.1 [141].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Path Coefficient Results

Hypotheses		Beta/OS	T-Value	P-Value	Decision
H1a	PV -> PI	0.164	2.736	0.006	Significant
H2a	PS -> PI	0.263	3.637	0.000	Significant
H3a	RE -> PI	0.016	0.350	0.726	Not Significant
H4a	RC -> PI	0.138	2.717	0.007	Significant
H5a	SSE -> PI	0.002	0.424	0.672	Not Significant
H6a	ATT -> PI	0.029	0.535	0.593	Not Significant
H7a	SN -> PI	0.015	2.471	0.014	Significant
H8a	PBC -> PI	0.131	2.037	0.042	Significant
H9a	ISA -> PI	-0.005	0.995	0.032	Not Significant
H10a	KNOW -> PI	0.121	2.152	0.032	Significant
H1b	PV -> PB	0.141	3.196	0.001	Significant
H2b	PS -> PB	0.332	6.000	0.000	Significant
H3b	RE -> PB	0.074	2.142	0.033	Significant
H4b	RC -> PB	0.121	3.745	0.000	Significant
H5b	SSE -> PB	-0.015	0.405	0.685	Not Significant
H6b	ATT -> PB	0.009	2.415	0.016	Significant
H7b	SN -> PB	0.125	2.551	0.011	Significant
H8b	PBC -> PB	0.082	2.251	0.025	Significant
H9b	ISA -> PB	-0.056	1.513	0.131	Not Significant
H10b	KNOW -> PB	-0.035	0.745	0.457	Not Significant
H11	PI -> PB	0.234	3.958	0.000	Significant

Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

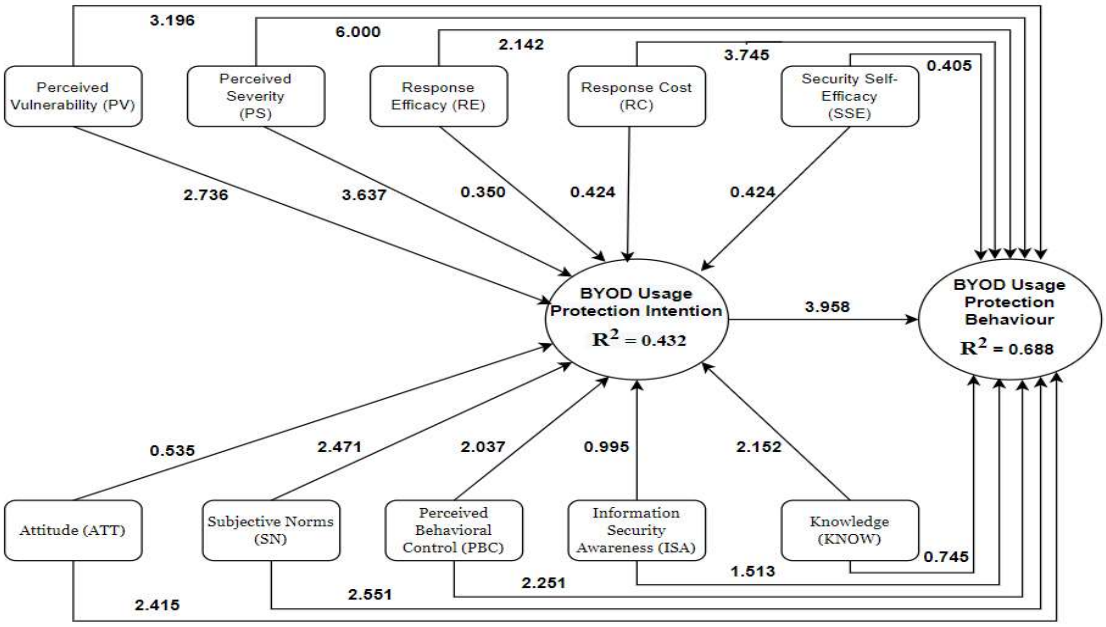

Figure 2: A Structural Research Model

5.2. Mediation Effect of Protection Intention (Indirect)

A bootstrapping approach was conducted to analyze the mediation relationships [142] of protection intention between perceived vulnerability, perceived severity, response efficacy, response cost, security self-efficacy, attitude, subjective norms, perceived behavior control, information security awareness, and knowledge. Table 2 presents the mediation analysis results. The results indicated that five of the 10 mediating hypotheses, H1c (PV -> PI-> PB, p =.041), H2c (PS -> PI -> PB, p = .012), H4c (RC -> PI -> PB, p = .03), H7c (SN -> PI -> PB, p = .044), and H10c (KNOW -> PI -> PB, p = .046) were statistically significant. Meanwhile, the other five hypotheses, namely H3c (RE -> PI -> PB, p = .739), H5c (SSE -> PI -> PB, p = .684), H6c (ATT -> PI -> PB, p = .620), H8c (PBC -> PI -> PB, p = .098), and H9c (ISA -> PI -> PB, p = .353) were statistically insignificant. The mediating route is statistically significant when p-values are less than 0.05, together with positive Lower Limit (LL) and Upper Limit (UL) values.

Table 2: Mediation Analysis Result

Hypotheses		Beta/OS	T-Value	P-Value	Decision
H1c	PV -> PI -> PB	0.038	2.052	0.041	Significant
H2c	PS -> PI -> PB	0.062	2.526	0.012	Significant
H3c	RE -> PI -> PB	0.004	0.334	0.739	Not Significant
H4c	RC -> PI -> PB	0.032	2.173	0.030	Significant
H5c	SSE -> PI -> PB	0.005	0.407	0.684	Not Significant
H6c	ATT -> PI -> PB	0.007	0.496	0.620	Not Significant
H7c	SN -> PI -> PB	0.035	2.021	0.044	Significant
H8c	PBC -> PI -> PB	0.031	1.659	0.098	Not Significant
H9c	ISA -> PI -> PB	0.012	0.930	0.353	Not Significant
H10c	KNOW -> PI -> PB	0.028	2.001	0.046	Significant

6. DISCUSSION

This study confirmed that both PMT and TPB theories can be accepted as a promising theoretical framework to understand the factors determining an employee's decision to engage in BYOD protection behaviors. Consistent with PMT, perceived vulnerability, perceived severity, and response cost were determined as significant determinants of the intentions to adopt BYOD protection behavior. Whereas, subjective norms and perceived behavioral control were significant determinants of the intentions to adopt BYOD protection behavior, consistent with TPB. The results also revealed that knowledge affected the protection intention of BYOD. It also indicated that the 'knowledge-attitude-behavior' theory is still accepted while planning strategies for employees to engage in BYOD protection behavior. Increased protection of BYOD knowledge can change a person's attitude to become more responsible in protecting their devices when performing their office work.

The significant effects of perceived vulnerability on both protection intention (H1a) and protection behavior (H1b) are in line with the findings from previous studies [23, 73]. If employees are aware that their devices are vulnerable to security threats, they are more likely to engage in protection behavior. Hence, the organizations should ensure that in a BYOD environment, employees are aware of the threats that might occur if they do not take cautionary actions to secure their devices. Similarly, the effects of perceived severity were also significant on both protection intention (H2a) and protection behavior (H2b). To increase an employee's engagement in protection behavior, an employee needs to be aware of the severity of the threats if they choose to not abide by the company's protection policies. [73] asserted that employees' awareness of the security threats or attacks their organisations may face as a result of any unsafe behavior that does not follow their organisations' security recommendations is an important determinant of their BYOD protection behavior. Meanwhile, the subjective norms factor significantly affected protection intention (H7a) and protection behavior (H7b) among the employees, reflecting the findings from previous studies [84, 63, 85]. The employees are influenced by their co-workers and superior's decisions on the use of BYOD and whether they should follow the organization's BYOD protection policies. Next, the perceived behavioral control also significantly influenced protection intention (H8a) and protection behavior (H8b) [86, 87]. The result indicated that the employees trust in their capabilities and skills to protect their own devices.

Based on the results, security self-efficacy was insignificant on BYOD protection intention (H5a) and protection behaviors (H5b), which contradicted our hypotheses. In short, this result implies that employees are confident in performing the necessary steps required to ensure the protection of using their own devices [61, 52]. Whereas, information security awareness had no significant effects on protection intention (H9a) and protection behavior (H9b). This result contradicted our hypothesis and findings from previous studies [92, 67]. This study indicated that employees have a good sense of awareness about the potential risks and security threats of using their own devices. On the other hand, although [65] revealed that response cost does not have a significant effect on protection intention and protection behavior, our study reported that response cost can significantly influence BYOD intention (H4a) and protection behaviors (H4b). These results revealed that employees are more aware of the efforts and time needed to keep their devices secure. Meanwhile, response efficacy was insignificant on protection intention (H3a) which contradicted with previous studies [77, 27, 76]. However, response efficacy can significantly influence protection behavior (H3b). It indicated that employees do perceive the importance of organizational protection policies and recommendations in their protection behavior towards BYOD usage. Similar to H3a, attitude was not significant towards protection intention (H6a) and protection behavior (H6b). These findings contradicted the findings of previous studies, which revealed that response efficacy and attitude can significantly influence protection intention and protection behavior (76; 77, 82]. The response efficacy towards protection behavior of BYOD implies that it is important for employees to understand the efficacy of taking protective actions and realizing their responsibility in protecting themselves in a BYOD environment. Whereas, the insignificant relationship between attitude and BYOD protection behaviors implied that the attitude of employees is not an important factor when deciding whether or not to engage in BYOD protection behavior. Regardless of their attitude (positive or negative), knowing the consequences of unsafe behavior is sufficient to make them engage in BYOD protection behavior. Meanwhile, the significance of knowledge on protection intention (H10a) and protection behavior (H10b) suggested that sufficient security-related knowledge such as threats and risks

of using BYOD could help instill security concern. This piece of knowledge will, in turn, lead to more engagement in BYOD protection intention, though it may not directly affect their behavior.

As predicted, intentions to perform protection behaviors can significantly influence actual protection behavior (H11). Employees who have the intention to protect their devices in a BYOD environment are more likely to engage in protection behavior. This finding also supported the utilisation of TPB as a model for the determinants of intention, demonstrating that perceived vulnerability, perceived severity, response cost, subjective norm, perceived behavioral control, and knowledge accounted for 43% of the variance in employees' intentions to protect their devices. Furthermore, the determinants of behavior (perceived vulnerability, perceived severity, response efficacy, response cost, attitude, subjective norm, and perceived behavioral control) accounted for 68% of the variance in employees' behavior to protect their devices.

Based on the mediation results, the mediation of protection intention yielded a significant mediation effect between perceived vulnerability, perceived severity, response cost, subjective norms, knowledge, and protection behavior. On the other hand, the mediation of protection intention between response efficacy, security self-efficacy, attitude, perceived behavior control, information security awareness, and protection behavior indicated no significant mediation effect. The results are consistent with previous studies [138, 121, 65, 139] which implied that intention is a good mediating variable between the independent variables and the outcome variable.

7. CONTRIBUTIONS, LIMITATIONS AND FUTURE RESEARCH

7.1. Theoretical Contributions

This study added to the corpus of information on the factors influencing the protection intention for BYOD usage protection behaviors. The following are four key theoretical contributions to this study. Firstly, this study was one of the first empirical studies to identify factors of BYOD protection intentions that influence BYOD protection behaviors. This conceptual model could help enterprises to better understand and deal with the determinants of BYOD protection intentions and their effects on employee behavior. Most of the previous studies were centered mainly on technological problems related to the implementation of BYOD without considering the human factor on information security and policies [44, 64, 145, 146]. According to [146], organizations need to understand that technical measures alone are insufficient to ensure information security. Secondly, this study integrated TPB with PMT as a relatively new conceptual model, by suggesting that both theories can be used to explain the BYOD usage protection behaviors. In this vein, this study lends further support to the important roles of these theories in understanding human behaviors in various contexts. Thirdly, the present study fills the gap in the limited information on BYOD protection. Next, the research provides primary the results of data collection that were not previously available as its important contribution as it allowed our conceptual model to be tested in a country (Oman) that is ranked differently in the middle east of the information security index. Therefore, it can be used for future comparative studies to address the determinants found in this study, namely, perceived vulnerability, perceived severity, response efficacy, response cost, attitude, subjective norm, perceived behavioral control, and security self-efficacy. Finally, this study proposed that protection intention mediates the effects of other variables adopted in this study on protection behaviors. The results from this study enhanced our understanding on the mediating role of protection intention, which is currently limited and was ignored in previous studies [121, 139].

7.2. Practical Contributions

By assessing the present condition of their employees' security behavior, businesses and information security managers can implement appropriate processes and procedures to reduce the associated risks of BYOD. Contrarily, the next generation of employees will support BYOD usage in an organization. This study also encourages employers and organizations to be more aware of adopting BYOD usage because employees see the potential benefits and want to exploit them, which leads to information leaking and BYOD usage risks. Therefore, employers need to develop a more responsive plan to avoid any protection issues. This study also assisted firms to get insight into strategic policy design, protection policy implementation, training planning, and an awareness program checklist to establish a strong security culture within their organizations. Furthermore, additional protection measures are needed for the information security unit. Employees must be informed of the consequences of their actions. Training and policies must be instituted before an unprecedented data leak

occurs.

The findings from this study are useful to policymakers and strategists since determining the causes of BYOD protection behaviors among employees could reduce the danger of data leakage, both purposefully and accidentally. Employers and organizations are responsible for securing the company data assets by ensuring BYOD usage protection. The BYOD utilization pattern is unavoidable, and it is presently not a choice. This study also expects to assist decision-makers in structuring their goals to install protection behavior determinants among personnel within firms. Increased BYOD usage security behavior among government personnel is required to boost the organization's performance.

The COVID-19 pandemic represents a chance for organizations and employers to establish strong protection of BYOD used by employees. Employers would be able to understand the influences on their employees' BYOD protection intention and behavior as the pandemic caused a major rotation direction as employees were allowed by their organizations to work remotely.

7.3. Limitations and Future Research

The study has two limitations that should be considered when interpreting the findings. Firstly, in addition to the variables used in this study, future studies should also include variables from other theories previously used in IS security, as they may improve the model's explanatory power of the protection behavior. Secondly, this study was conducted on an individual level, hence, future studies could assess the organizational level to enhance the strategies for BYOD protection policy at both individual and organizational levels. Thirdly, one of the significant recommendations in this study is to interpret and capture the rich data because one of the limitations of this study has relied only on a quantitative approach. It is beneficial that in future research, the implications of the impacts found in the current research to significant employers of the organizations by performing the qualitative approach of data collection and analysis could be included in future studies to obtain data in different forms.

8. CONCLUSION

This study aimed to identify and assess the determinants of BYOD use protection intentions, which in turn influence BYOD usage protection behaviors. The determinants were examined through the developed conceptual model for protection intentions towards BYOD usage that influences BYOD usage protection behavior. PLS-SEM was used to test the proposed conceptual model in a cross-sectional survey. Limitations and recommendations for future research were also discussed. Overall, this study contributes as one of the first milestones in addressing the BYOD security issues among employees by understanding the determinants of BYOD protection behavior.

REFERENCES

[1] A. Weeger *et al.*, "Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives," *Inf. Syst. Front.*, vol. 22, no. 1, pp. 1–17, 2020, doi: 10.1007/s10796-018-9857-4.

[2] Hughes, "BYOD and the Medical Practice." 2016.

[3] S. Vrhovec and B. Markelj, "Relating mobile device use and adherence to information security policy with data breach consequences in hospitals," *J. Univers. Comput. Sci.*, vol. 24, no. 5, pp. 634–645, 2018.

[4] S. K. Preeti Wadhwani, "Bring Your Own Device (BYOD) Market Size to exceed $ 300bn by 2022," 2019, [Online]. Available: https://www.gminsights.com/pressrelease/bring-your-own-device-byod-market-report.

[5] M. S. Doargajudhur and P. Dell, "The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation," *J. Comput. Inf. Syst.*, vol. 00, no. 00, pp. 1–12, 2018, doi: 10.1080/08874417.2018.1543001.

[6] C. A. Agudelo, R. Bosua, A. Ahmad, and S. B. Maynard, "Understanding knowledge leakage & BYOD (bring your own device): A mobile worker perspective," *ACIS 2015 Proc. - 26th Australas. Conf. Inf. Syst.*, pp. 1–13, 2016, [Online]. Available: https://arxiv.org/abs/1606.01450.

[7] Forcepoint, "What is Spoofing?," *Forcepoint*, pp. 1–7, 2020, [Online]. Available: https://www.forcepoint.com/cyber-edu/spoofing.

[8] Europol, "Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain," *Europol*, no. March, pp. 19–21, 2018, [Online]. Available: https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain.

[9] L. Weber and R. J. Rudman, "Addressing the incremental risks associated with adopting Bring Your Own Device," *J. Econ. Financ. Sci.*, vol. 11, no. 1, pp. 1–13, 2018, doi: 10.4102/jef.v11i1.169.

[10] Jeff Pochepan, "Employees Working On Their Personal Devices? Here's How You Can Protect Your Business Data." 2018, [Online]. Available: https://www.inc.com/jeff-pochepan/employees-working-on-their-personal-devices-heres-how-you-can-protect-your-business-data.html.

[11] K. Almarhabi, K. Jambi, F. Eassa, and O. Batarfi, "A Proposed Framework for Access Control in the Cloud and BYOD Environment," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 2, pp. 144–152, 2018, doi: 10.1016/j.compchemeng.2004.08.038.

[12] D. M. and J. A. Abubakar Garba Bello, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments," *Inf. andComputer Secur.*, vol. 23, no. 5, pp. 450–475, 2017, doi: 10.1111/1365-2664.12960.

[13] M. Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)," *Phys. Procedia*, vol. 78, no. December 2015, pp. 179–184, 2016, doi: 10.1016/j.procs.2016.02.030.

[14] B. Alotaibi and H. Almagwashi, "A Review of BYOD Security Challenges, Solutions and Policy Best Practices," *1st Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2018*, pp. 1–6, 2018, doi: 10.1109/CAIS.2018.8441967.

[15] M. M. Ratchford and Y. Wang, "Byod-insure: A security assessment model for enterprise byod," *2019 5th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2019*, pp. 1–10, 2019, doi: 10.1109/MOBISECSERV.2019.8686551.

[16] F. Belanger and R. E. Crossler, "Dealing with digital traces: Understanding protective behaviors on mobile devices," *J. Strateg. Inf. Syst.*, vol. 28, no. 1, pp. 34–49, 2019, doi: 10.1016/j.jsis.2018.11.002.

[17] M. Alohali, N. Clarke, S. Furnell, and S. Albakri, "Information security behavior: Recognizing the influencers," *Proc. Comput. Conf. 2017*, vol. 2018-Janua, no. July, pp. 844–853, 2018, doi: 10.1109/SAI.2017.8252194.

[18] M. Mahinderjit, C. Wai, and Z. Zulkefli, "Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 53–62, 2017, doi: 10.14569/IJACSA.2017.080208.

[19] P. M. Kaspersky and M. Woburn, "Kaspersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices," pp. 19–22, 2018.

[20] S. Allam, S. V. Flowerday, and E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," *Comput. Secur.*, vol. 42, pp. 56–65, 2014, doi: 10.1016/j.cose.2014.01.005.

[21] A. Koohang, K. Floyd, N. Rigole, and J. Paliszkiewicz, "Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs," *Online J. Appl. Knowl. Manag.*, vol. 6, no. 2, pp. 7–22, 2018, doi: 10.36965/ojakm.2018.6(2)7-22.

[22] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manage.*, vol. 45, no. October 2018, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[23] N. Ameen, A. Tarhini, M. H. Shah, N. Madichie, J. Paul, and J. Choudrie, "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce," *Comput. Human Behav.*, vol. 114, no. April 2020, p. 106531, 2021, doi: 10.1016/j.chb.2020.106531.

[24] R. Palanisamy, A. A. Norman, and M. L. M. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Comput. Secur.*, vol. 98, 2020, doi: 10.1016/j.cose.2020.101998.

[25] K. Timms, "BYOD must be met with a wider appreciation of the cyber-security threat," *Comput. Fraud Secur.*, vol. 2017, no. 7, pp. 5–8, 2017, doi: 10.1016/S1361-3723(17)30058-1.

[26] C. L. Anderson and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 613–643, 2010, doi: 10.2307/25750694.

[27] M. Warkentin, A. C. Johnston, J. Shropshire, and W. D. Barnett, "Continuance of protective security behavior: A longitudinal study," *Decis. Support Syst.*, vol. 92, pp. 25–35, 2016, doi: 10.1016/j.dss.2016.09.013.

[28] H. U. Khan and K. A. AlShare, "Violators versus non-violators of information security measures in organizations—A study of distinguishing factors," *J. Organ. Comput. Electron. Commer.*, vol. 29, no. 1, pp. 4–23, 2019, doi: 10.1080/10919392.2019.1552743.

[29] R. Chakraborty, J. Lee, S. Bagchi-Sen, S. Upadhyaya, and H. Raghav Rao, *Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults*, vol. 83, no. 2016. Elsevier B.V., 2016.

[30] Oberlo, "How Many People Have Smartphones in Number of Smartphone Users in Advanced and Emerging Economies," 2020.

[31] Ash Turner, "HOW MANY SMARTPHONES ARE IN THE WORLD ? September 2021 Mobile User Statistics," no. Sept, pp. 1–23, 2021, [Online]. Available: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.

[32] C. Lellis, "Mobile Devices in the Workplace: 40 Statistics You Should Know in 2021," pp. 1–11, 2021, [Online]. Available: http://www.perillon.com/blog/mobile-statistics-devices-at-work.

[33] A. Government, *Bring Your Own Device : A Guide for Schools*. 2012.

[34] Beyond Identity, "BYOD: Exploring the Evolution of Work Device Practices in a New Remote-Forward Era [Survey]," *Beyond Identity Blog*, pp. 1–14, 2021, [Online]. Available: https://www.beyondidentity.com/blog/byod-exploring-evolution-work-device-practices-survey.

[35] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, p. 102248, 2021, doi: 10.1016/j.cose.2021.102248.

[36] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic," *J. Med. Internet Res.*, vol. 22, no. 9, pp. 7–10, 2020, doi: 10.2196/23692.

[37] M. S. Doargajudhur and P. Dell, "Impact of BYOD on organizational commitment: an empirical investigation," *Inf. Technol. People*, vol. 32, no. 2, pp. 246–268, 2019, doi: 10.1108/ITP-11-2017-0378.

[38] P. Baillette, Y. Barlette, and A. Leclercq-Vandelannoitte, "Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users," *Int. J. Inf. Manage.*, vol. 43, no. July, pp. 76–84, 2018, doi: 10.1016/j.ijinfomgt.2018.07.007.

[39] S. Köffer, K. Ortbach, I. Junglas, B. Niehaves, and J. Harris, "Innovation Through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior," *Bus. Inf. Syst. Eng.*, vol. 57, no. 6, pp. 363–375, 2015, doi: 10.1007/s12599-015-0387-z.

[40] G. M, "Navigating Collaboration Risks and Challenges in a BYOD Culture," pp. 1–6, 2018, [Online]. Available: https://www.neweratech.com/us/blog/navigating-collaboration-risks-and-challenges-in-a-byod-culture/.

[41] S. Blizzard, "Coming full circle: Are there benefits to BYOD?," *Comput. Fraud Secur.*, vol. 2015, no. 2, pp. 18–20, 2015, doi: 10.1016/S1361-3723(15)30010-5.

[42] O. U. Franklin and M. Ismail Z., "the Future of Byod in Organizations and Higher Institution of Learning," *Int. J. Inf. Syst. Eng.*, vol. 3, no. 1, pp. 110–128, 2017, doi: 10.24924/ijise/2015.11/v3.iss1/110.128.

[43] M. Eiza, R. I. Okeke, J. Dempsey, and V.-T. Ta, "Keep Calm and Carry on with Cybersecurity @Home: A Framework for Securing Homeworking IT Environment," *Int. J. Cyber Situational Aware.*, vol. 5, no. 1, pp. 1–25, 2021, doi: 10.22619/ijcsa.2020.100131.

[44] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, "BYOD Policy Compliance: Risks and Strategies in Organizations," *J. Comput. Inf. Syst.*, vol. 00, no. 00, pp. 1–12, 2020, doi: 10.1080/08874417.2019.1703225.

[45] C. H. Goh and A. P. Teoh, "DETERMINING BRING YOUR OWN DEVICE (BYOD) SECURITY POLICY COMPLIANCE AMONG MALAYSIAN TELEWORKERS: PERCEIVED CYBERSECURITY GOVERNANCE AS MODERATOR," pp. 305–310, 2021, [Online]. Available: https://ieeexplore.ieee.org/document/9655895.

[46] B. N-able, "The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember The rise of BYOD What this means For MSPs Top BYOD risks," pp. 1–5, 2021, [Online]. Available: https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember#:~:text=Data theft,corporate data and confidential information.

[47] and R. O. S. Melva Ratchford, Ping Wang, *BYOD Security Risks and Mitigations*, vol. 558. 2018.

[48] Ronald W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude," 1975. https://www-tandfonline-com.ezproxy.uniten.edu.my/doi/abs/10.1080/00223980.1975.9915803.

[49] S. Aurigemma and T. Mattson, "Exploring the effect of uncertainty avoidance on taking voluntary protective security actions," *Comput. Secur.*, vol. 73, pp. 219–234, 2018, doi: 10.1016/j.cose.2017.11.001.

[50] R. Floyd, D.L., Prentice-Dunn, S. and Rogers, "A meta-analysis of research on protection motivation theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 2, pp. 407–429, 2000.

[51] Tejaswini Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[52] A. J. Burns, C. Posey, T. L. Roberts, and P. Benjamin Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals," *Comput. Human Behav.*, vol. 68, pp. 190–209, 2017, doi: 10.1016/j.chb.2016.11.018.

[53] Y. Lee and K. A. Kozar, "An empirical investigation of anti-spyware software adoption: A multitheoretical perspective," *Inf. Manag.*, vol. 45, no. 2, pp. 109–119, 2008, doi: 10.1016/j.im.2008.01.002.

[54] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008, doi: 10.1016/j.chb.2008.04.005.

[55] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012, doi: 10.1016/j.im.2012.04.002.

[56] A. D. Giwah, L. Wang, Y. Levy, and I. Hur, "Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory," *J. Intellect. Cap.*, vol. 21, no. 2, pp. 215–233, 2020, doi: 10.1108/JIC-03-2019-0063.

[57] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Q. Manag. Inf. Syst.*, vol. 39, no. 4, pp. 837–864, 2015, doi: 10.25300/MISQ/2015/39.4.5.

[58] C. Posey, T. L. Roberts, and P. B. Lowry, "The impact of organizational commitment on insiders motivation to protect organizational information assets," *J. Manag. Inf. Syst.*, vol. 32, no. 4, pp. 179–214, 2015, doi: 10.1080/07421222.2015.1138374.

[59] S. Prentice-Dunn, B. F. McMath, and R. J. Cramer, "Protection motivation theory and stages of change in sun protective behavior," *J. Health Psychol.*, vol. 14, no. 2, pp. 297–305, 2009, doi: 10.1177/1359105308100214.

[60] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012, doi: 10.1016/j.cose.2011.10.007.

[61] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Comput. Secur.*, vol. 48, pp. 281–297, 2015, doi: 10.1016/j.cose.2014.11.002.

[62] B. Hanus and Y. "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 2–16, 2016, doi: 10.1080/10580530.2015.1117842.

[63] N. Thompson, T. J. McGill, and X. Wang, "'Security begins at home': Determinants of home computer and mobile device security behavior," *Comput. Secur.*, vol. 70, pp. 376–391, 2017, doi: 10.1016/j.cose.2017.07.003.

[64] A. Duke Giwah, "User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2018-April, pp. 1–5, 2018, doi: 10.1109/SECON.2018.8479178.

[65] S. F. Verkijika, "Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret," *Comput. Secur.*, vol. 77, pp. 860–870, 2018, doi: 10.1016/j.cose.2018.03.008.

[66] J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware

behaviours," *Comput. Human Behav.*, vol. 87, no. May, pp. 87–97, 2018, doi: 10.1016/j.chb.2018.05.023.

[67] G. A. Duke, W. Ling, L. Yair, and H. Inkyoung, "Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory," *Journal of Intellectual Capital*, vol. ahead-of-p, no. ahead-of-print. Jan. 01, 2019, doi: 10.1108/JIC-03-2019-0063.

[68] Zhiling, J. Adkins, and G. Y. Zhao, "Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory," *MWAIS 2018 Proc.*, vol. 2019, no. 1, p. 25, 2019, doi: 10.17705/3jmwa.000045.

[69] N. Ameen, A. Tarhini, M. Hussain Shah, and N. O. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study," *Comput. Human Behav.*, vol. 104, p. 106184, 2020, doi: 10.1016/j.chb.2019.106184.

[70] V. Cho and W. H. Ip, "A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy," *Enterp. Inf. Syst.*, vol. 12, no. 6, pp. 659–673, 2018, doi: 10.1080/17517575.2017.1404132.

[71] E. M. Rogers, "Diffusion of Innovations: Modifications of a Model for Telecommunications," *Die Diffus. von Innov. der Telekommunikation*, pp. 25–38, 1995, doi: 10.1007/978-3-642-79868-9_2.

[72] R. S. Lazarus, "The Stress Concept in the Life Sciences," 1984, [Online]. Available: https://books.google.com.om/books?hl=en&lr=&id=i-ySQQuUpr8C&oi=fnd&pg=PR5&dq=Lazarus,+R.+S.+(1984).+Stress,+Appraisal,+and+Coping&ots=DgGSprlkSe&sig=sRtj7JcSZj7GKXA2XPKB7KXDIVU&redir_esc=y#v=onepage&q=Lazarus%2C R. S. (1984). Stress%2C Appraisal%2C and Co.

[73] H. L. Chou and C. Chou, "An analysis of multiple factors relating to teachers' problematic information security behavior," *Comput. Human Behav.*, vol. 65, pp. 334–345, 2016, doi: 10.1016/j.chb.2016.08.034.

[74] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti, "Privacy calculus model in e-commerce - A study of Italy and the United States," *Eur. J. Inf. Syst.*, vol. 15, no. 4, pp. 389–402, 2006, doi: 10.1057/palgrave.ejis.3000590.

[75] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Comput. Human Behav.*, vol. 28, no. 6, pp. 2366–2375, 2012, doi: 10.1016/j.chb.2012.07.008.

[76] I. Topa and M. Karyda, "Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9264, no. September, p. 5, 2015, doi: 10.1007/978-3-319-22906-5.

[77] S. R. C. Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput. Secur.*, vol. 59, no. 1318885, pp. 138–150, 2016, doi: 10.1016/j.cose.2016.02.009.

[78] A. Noushin, L. Daniel, K. Jean-Pierre, and S. G. Christoph, "An integrated framework to examine mobile users' pathway from threat cognition to action," *7th Int. Symp. Digit. Forensics Secur. ISDFS 2019*, 2019, doi: 10.1109/ISDFS.2019.8757556.

[79] Z. Tu, O. Turel, Y. Yuan, and N. Archer, "Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination," *Inf. Manag.*, vol. 52, no. 4, pp. 506–517, 2015, doi: 10.1016/j.im.2015.03.002.

[80] S. Hina and D. D. Dominic, "Need for information security policies compliance: A perspective in Higher Education Institutions," *Int. Conf. Res. Innov. Inf. Syst. ICRIIS*, pp. 1–6, 2017, doi: 10.1109/ICRIIS.2017.8002439.

[81] S. Dhawan, K. Singh, and S. Goel, "Impact of privacy attitude, concern and awareness on use of online social networking," *Proc. 5th Int. Conf. Conflu. 2014 Next Gener. Inf. Technol. Summit*, pp. 14–17, 2014, doi: 10.1109/CONFLUENCE.2014.6949226.

[82] A. Nasir, R. Abdullah Arshah, and M. R. Ab Hamid, "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," *Inf. Secur. J. A Glob. Perspect.*, vol. 28, no. 3, pp. 55–80, 2019, doi: 10.1080/19393555.2019.1643956.

[83] M. Martens, R. De Wolf, and L. De Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general," *Comput. Human*

Behav., vol. 92, no. May 2018, pp. 139–150, 2019, doi: 10.1016/j.chb.2018.11.002.

[84] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care beour formation in organizationshavi," *Comput. Secur.*, vol. 53, pp. 65–78, 2015, doi: 10.1016/j.cose.2015.05.012.

[85] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Comput. Secur.*, vol. 80, pp. 211–223, 2019, doi: 10.1016/j.cose.2018.09.016.

[86] F. Husain, M. G. Shahnawaz, N. H. Khan, H. Parveen, and K. Savani, "Intention to get COVID-19 vaccines: Exploring the role of attitudes, subjective norms, perceived behavioral control, belief in COVID-19 misinformation, and vaccine confidence in Northern India," *Hum. Vaccines Immunother.*, vol. 00, no. 00, pp. 1–13, 2021, doi: 10.1080/21645515.2021.1967039.

[87] İ. Dilekler, C. Doğulu, and Ö. Bozo, "A test of theory of planned behavior in type II diabetes adherence: The leading role of perceived behavioral control," *Curr. Psychol.*, vol. 40, no. 7, pp. 3546–3555, 2021, doi: 10.1007/s12144-019-00309-7.

[88] E. Andarge *et al.*, "Intention and practice on personal preventive measures against the covid-19 pandemic among adults with chronic conditions in southern ethiopia: A survey using the theory of planned behavior," *J. Multidiscip. Healthc.*, vol. 13, pp. 1863–1877, 2020, doi: 10.2147/JMDH.S284707.

[89] J. Kaur, N. Mustafa, Kaur, and Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," *Int. Conf. Res. Innov. Inf. Syst. ICRIIS*, vol. 2013, pp. 286–290, 2013, doi: 10.1109/ICRIIS.2013.6716723.

[90] A. McCormac, D. Calic, M. Butavicius, K. Parsons, T. Zwaans, and M. Pattinson, "A reliable measure of Information Security Awareness and the identification of bias in responses," *Australas. J. Inf. Syst.*, vol. 21, pp. 1–12, 2017, doi: 10.3127/ajis.v21i0.1697.

[91] J. Ortiz, S. H. Chang, W. H. Chih, and C. H. Wang, "The contradiction between self-protection and self-presentation on knowledge sharing behavior," *Comput. Human Behav.*, vol. 76, pp. 406–416, 2017, doi: 10.1016/j.chb.2017.07.031.

[92] T. Sommestad, H. Karlzén, and J. Hallberg, "The Theory of Planned Behavior and Information Security Policy Compliance," *J. Comput. Inf. Syst.*, vol. 59, no. 4, pp. 344–353, 2019, doi: 10.1080/08874417.2017.1368421.

[93] T. Baranowski, K. W. Cullen, T. Nicklas, D. Thompson, and J. Baranowski, "Are current health behavioral change models helpful in guiding prevention of weight gain efforts?," *Obes. Res.*, vol. 11, no. SUPPL. 1, 2003, doi: 10.1038/oby.2003.222.

[94] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[95] S. H. Lim, "An Investigation of the Psychology of Password Replacement by Email Users," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 26, no. 5, pp. 1251–1258, 2016, doi: 10.13089/jkiisc.2016.26.5.1251.

[96] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, no. May, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[97] A. Musarurwa, S. Flowerday, and L. Cilliers, "An information security behavioural model for the bring-your-own-device trend," *SA J. Inf. Manag.*, vol. 20, no. 1, pp. 1–9, 2018, doi: 10.4102/sajim.v20i1.980.

[98] R. E. Crossler and F. Bélanger, "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors," *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, pp. 4071–4080, 2017, doi: 10.24251/hicss.2017.491.

[99] A. Gurung and M. K. Raja, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," *Inf. Comput. Secur.*, vol. 24, no. 4, pp. 348–371, 2016, doi: https://doi.org/10.1108/ICS-05-2015-0020.

[100] B. C. L. Anderson, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," vol. 34, no. 3, pp. 613–643, 2010, [Online]. Available: https://www.jstor.org/stable/25750694.

[101] S. Milne, S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," pp. 163–184,

2002, [Online]. Available: internal-pdf://0719885367/Milne_et_al-2002-British_Journal_of_Health_Psy.pdf.

[102] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: A model of online protection behaviour," *Behav. Inf. Technol.*, vol. 27, no. 5, pp. 445–454, 2008, doi: 10.1080/01449290600879344.

[103] W. P. Wong, H. C. Tan, K. H. Tan, and M. L. Tseng, "Human factors in information leakage: mitigation strategies for information sharing integrity," *Ind. Manag. Data Syst.*, vol. 119, no. 6, pp. 1242–1267, 2019, doi: 10.1108/IMDS-12-2018-0546.

[104] A. M. Kelly, T. Shimeall, J. Blando, C. Member, R. Valentine, and T. C. Wilson, "The Ability To Protect Against Insider Threats Introduced Via Bring Your Own Device," 2020, [Online]. Available: https://www.proquest.com/openview/8adaba293b127ba7636f831ebe230498/1?pq-origsite=gscholar&cbl=44156.

[105] M. H. Jarrahi, K. Crowston, K. Bondar, and B. Katzy, "A pragmatic approach to managing enterprise IT infrastructures in the era of consumerization and individualization of IT," *Int. J. Inf. Manage.*, vol. 37, no. 6, pp. 566–575, 2017, doi: 10.1016/j.ijinfomgt.2017.05.016.

[106] A. N. Albarq and A. Alsughayir, "Examining Theory of Reasoned Action in Internet Banking Using SEM among Saudi Consumers," *Int. J. Mark. Pract.*, vol. 1, no. 1, pp. 16–30, 2013, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2270448.

[107] J. L. Chiu, N. C. Bool, and C. L. Chiu, "Challenges and factors influencing initial trust and behavioral intention to use mobile banking services in the Philippines," *Asia Pacific J. Innov. Entrep.*, vol. 11, no. 2, pp. 246–278, 2017, doi: 10.1108/apjie-08-2017-029.

[108] M. Fishbein and I. Ajzen, "Belief, attitude, intention, and behavior: An introduction to theory and research," *J. Bus. Ventur.*, vol. 5, no. 3, pp. 177–189, 1975, doi: 10.1016/0883-9026(90)90031-N.

[109] I. Ajzen, "Behavioral Interventions Based on the Theory of Planned Behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1996, doi: 10.1016/0749-5978(91)90020-T.

[110] S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," *Inf. Syst. Res.*, vol. 6, no. 2, pp. 144–176, 1995, doi: 10.1287/isre.6.2.144.

[111] H. Ajjan and R. Hartshorne, "Investigating faculty decisions to adopt Web 2.0 technologies: Theory and empirical tests," *Internet High. Educ.*, vol. 11, no. 2, pp. 71–80, 2008, doi: 10.1016/j.iheduc.2008.05.002.

[112] A. A. Alalwan, Y. K. Dwivedi, and N. P. Rana, "Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust," *Int. J. Inf. Manage.*, vol. 37, no. 3, pp. 99–110, 2017, doi: 10.1016/j.ijinfomgt.2017.01.002.

[113] I. Arpaci, "Understanding and predicting students' intention to use mobile cloud storage services," *Comput. Human Behav.*, vol. 58, pp. 150–157, 2016, doi: 10.1016/j.chb.2015.12.067.

[114] J. Yang and Y. Zhang, "QR codes and authentication protection," *Wirel. Telecommun. Symp.*, vol. 2015-Janua, pp. 1–7, 2015, doi: 10.1109/WTS.2015.7117256.

[115] S. Y. Yousafzai, "A literature review of theoretical models of Internet banking adoption at the individual level," *J. Financ. Serv. Mark.*, vol. 17, no. 3, pp. 215–226, 2012, doi: 10.1057/fsm.2012.19.

[116] I. Ajzen and T. J. Madden, "Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control," *J. Exp. Soc. Psychol.*, vol. 22, no. 5, pp. 453–474, 1986, doi: 10.1016/0022-1031(86)90045-4.

[117] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: A model of online protection behavior," *Behav. Inf. Technol.*, vol. 27, no. 5, pp. 445–454, 2008, [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/01449290600879344?casa_token=T4ko_1pXePgAAAAA%3AdgR5AZnrvXKvFOYq9Zoo8PsO248jmzB9N8JY00tpwuajVKUJxDAnfDKMM2q6dExrDVAswH2yR9O9.

[118] SEOUNMI YOUN, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *Seounmi J. Consum. Aff. Fall*, vol. 43, no. 3, pp. 389–418, 2009, [Online]. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-6606.2009.01146.x.

[119] B. Han, "User's Information Security Awareness in BYOD Programs: A Theoretical Model," pp. 1–6, 2017, [Online]. Available: http://029e2c6.netsolhost.com/II-

Proceedings/2017/IIVC2017_HAN.pdf.
[120] S. Mafabi, S. Nasiima, E. M. Muhimbise, F. Kasekende, and C. Nakiyonga, "The mediation role of intention in knowledge sharing behavior," *VINE J. Inf. Knowl. Manag. Syst.*, vol. 47, no. 2, pp. 172–193, 2017, doi: 10.1108/VJIKMS-02-2016-0008.
[121] NCSI, "National Center for Statistics and Information Report," no. 02, 2021, doi: 10.46501/ijmtst0702.
[122] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*. 2007.
[123] B. M. Byrne, "Structural Equation Modeling With AMOS, EQS, and LISREL: Comparative Approaches to Testing for the Factorial Validity of a Measuring Instrument," *Int. J. Test.*, vol. 1, no. 1, pp. 55–86, 2001, doi: 10.1207/s15327574ijt0101_4.
[124] M. Götz, O., Liehr-Gobbers, K., & Krafft, *The evaluation of structural equation models and hypothesis testing. Principles of marketing research*. 2010.
[125] J. C. and B. Nunnally, "Book Review: Psychometric theory," *J. Psychoeduc. Assess.*, vol. 17, no. 3, pp. 275–280, 1994, doi: 10.1177/073428299901700307.
[126] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951, doi: 10.1007/BF02310555.
[127] C. Fornell and D. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Adv. Methods Mark. Res.*, vol. 18, no. 3, pp. 382-388., 1981, [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/002224378101800104.
[128] A. Musarurwa, S. Flowerday, and L. Cilliers, "The bring-your-own-device unintended administrator: A perspective from Zimbabwe," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 85, no. 4, pp. 1–20, 2018, doi: 10.1002/isd2.12076.
[129] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009, doi: 10.1287/isre.1070.0160.
[130] F. J. Haeussinger and J. J. Kranz, "INFORMATION SECURITY AWARENESS: ITS ANTECEDENTS AND MEDIATING EFFECTS ON SECURITY COMPLIANT BEHAVIOR," *Thirty Fourth Int. Conf. Inf. Syst.*, pp. 1–16, 2013, [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf.
[131] Y. Chen, C. Liang, and D. Cai, "Understanding WeChat Users' Behavior of Sharing Social Crisis Information," *Int. J. Hum. Comput. Interact.*, vol. 34, no. 4, pp. 356–366, 2018, doi: 10.1080/10447318.2018.1427826.
[132] L. Zhao, J. Yin, and Y. Song, "An exploration of rumor combating behavior on social media in the context of social crises," *Comput. Human Behav.*, vol. 58, pp. 25–36, 2016, doi: 10.1016/j.chb.2015.11.054.
[133] B. S. Chon, J. K. Lee, H. Jeong, J. Park, and J. Park, "Determinants of the Intention to Protect Personal Information among Facebook Users:," *ETRI J.*, vol. 40, no. 1, pp. 146–155, 2018, doi: 10.4218/etrij.2017-0082.
[134] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS," vol. 34, no. 3, pp. 523–548, 2010, [Online]. Available: https://www.jstor.org/stable/25750690.
[135] F. Putri and A. Hovav, "Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory," *ECIS 2014 Proc. - 22nd Eur. Conf. Inf. Syst.*, pp. 1–17, 2014, [Online]. Available: https://aisel.aisnet.org/ecis2014/proceedings/track16/2/.
[136] D. Straub and D. Gefen, "Validation Guidelines for IS Positivist Research," *Commun. Assoc. Inf. Syst.*, vol. 13, no. March, 2004, doi: 10.17705/1cais.01324.
[137] W. W. Chin, "The partial least squares approach to structural equation modelling," *Mod. Methods Bus. Res.*, vol. 295, no. 2, pp. 295–336, 1998, [Online]. Available: https://books.google.com.om/books?hl=en&lr=&id=EDZ5AgAAQBAJ&oi=fnd&pg=PA295&dq=The+partial+least+squares+approach+to+structural+equation+modelling&ots=49tG6qs4hp&sig=WGE10qfd58L6aQPk4icmKVDqcdM&redir_esc=y#v=onepage&q=The partial least squares approach to.
[138] A. Alfons, N. Y. Ateş, and P. J. F. Groenen, "A Robust Bootstrap Test for Mediation Analysis," *Organ. Res. Methods*, pp. 1–27,

2021, doi: 10.1177/1094428121999096.
[139] P. E. Shrout and N. Bolger, "Mediation in experimental and nonexperimental studies: New procedures and recommendations," *Psychol. Methods*, vol. 7, no. 4, pp. 422–445, 2002, doi: 10.1037/1082-989X.7.4.422.
[140] A. F. Hayes, "Beyond Baron and Kenny: Statistical mediation analysis in the new millennium," *Commun. Monogr.*, vol. 76, no. 4, pp. 408–420, 2009, doi: 10.1080/03637750903310360.
[141] M. Wetzels, G. Odekerken-Schröder, and C. Van Oppen, "Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration," *MIS Q. Manag. Inf. Syst.*, vol. 33, no. 1, pp. 177–196, 2009, doi: 10.2307/20650284.
[142] J. Kim, K. Merrill, and H. Yang, "Why we make the choices we do: Social TV viewing experiences and the mediating role of social presence," *Telemat. Informatics*, vol. 45, no. August, p. 101281, 2019, doi: 10.1016/j.tele.2019.101281.
[143] M. Sarstedt, C. M. Ringle, and J. F. Hair, *Partial least squares structural equation modeling*, no. September. 2017.
[144] Ghilan Al-Madhagy Taufiq-Hail, Shafiz Mohd Yusof, Ramadhan Abdo Musleh Alsaidi, Saleh R. Alanazi, *Collaborative and Social Media SaaS (Software as a Service) Cloud Computing Services' Adoption and Acceptance Model on the Millennials: Conceptual Model*, Studies in. The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success, 2021.
[145] B. Hauer, "Data and information leakage prevention within the scope of information security," *IEEE Access*, vol. 3, pp. 2554–2565, 2015, doi: 10.1109/ACCESS.2015.2506185.
[146] T. Grassegger and D. Nedbal, "The role of employees' information security awareness on the intention to resist social engineering," *Procedia Comput. Sci.*, vol. 181, no. 2019, pp. 59–66, 2021, doi: 10.1016/j.procs.2021.01.103.

Appendix A: Measurement Items

Measurement item	Loading	CA	CR	AVE
Attitude [51, 23, 97]		0.9	0.926	0.719
ATT1: I believe that it is beneficial for an organization to establish clear BYOD security policies, practices, and technologies.	0.909			
ATT2: I believe that it is useful for an organization to enforce its BYOD security policies, practices, and technologies.	0.815			
ATT3: I believe that it is a good idea for an organization to establish clear BYOD security policies, practices, and technologies.	0.927			
ATT4: If I am aware of my organization's sensitive nature and systems if managed well, BYOD's advantages outweigh the risks in today's modern technological era.	0.922			
ATT5: I believe that personal devices are being optimally managed within my organization to maximize their benefits while mitigating information security risks.	0.628			
Information Security Awareness [129, 130, 84]		0.911	0.926	0.61
ISA1: My organization provides training to help employees improve their awareness of personal device information security issues.	0.758			
ISA2: My organization provides employees with education on personal device software copyright laws.	0.783			
ISA3: In my organization, employees are briefed on the consequences of modifying BYOD data in an unauthorized way.	0.839			
ISA4: My organization educates employees on their personal device security responsibilities.	0.788			
ISA5: In my organization, employees are briefed on the consequences of accessing BYOD that they are not authorized to use.	0.82			
ISA6: I have sufficient knowledge about the cost of information security breaches when using my personal device.	0.837			
ISA7: I understand the risk of information security incidents when using my personal device.	0.726			
ISA8: I keep myself updated in terms of information security awareness when using my personal device.	0.697			
Knowledge [64, 128]		0.905	0.922	0.668
KNOW1: I have sufficient knowledge to protect organization data when using my personal device.	0.903			
KNOW2: Using a personal device at work would allow me access to all the information I require in order to perform my job satisfactorily.	0.745			
KNOW3: I have sufficient knowledge to process the protection when using my personal device.	0.933			
KNOW4: I am well informed about how to deal with problems caused by the organization's data when using my personal device.	0.921			
KNOW5: There is a growing demand from employees for the use of personal devices in the organization environment to allow unmonitored access to information and systems.	0.752			
KNOW6: Organizations that allow employees to bring their own devices are more information security-conscious than those that do not.	0.591			

Protection Behavior [23, 63]		0.866	0.909	0.716
PB1: I comply with personal devices protection recommendations.	0.868			
PB2: I do my best to follow personal devices protection rules and procedures strictly.	0.741			
PB3: I am certain that I will follow organizational, personal device protection recommendations (if they exist).	0.875			
PB4: My personal device is secured by a password.	0.892			
Perceived Behavioral Control [131, 132, 84]		0.901	0.924	0.669
PBC1: I think it's easy for me to share organizational information by using my personal device.	0.852			
PBC2: I am confident that if I want, I can share organizational information by using my personal device.	0.782			
PBC3: I have time, resources and knowledge to share organizational information by using my personal device.	0.867			
PBC4: I believe that information security-conscious care behavior is not a problematic practice when using my personal device.	0.821			
PBC5: I believe that my experiences help me have careful behavior about information security when using my personal device.	0.793			
PBC6: Following information security policies and procedures is easy for me when using my personal device.	0.788			
Protection Intention [133, 134, 16]		0.925	0.941	0.728
PI1: I will set the protection of personal information to maintain privacy during the use of my personal device.	0.889			
PI2: I do not want to disclose personal information when using my personal device.	0.813			
PI3: I will limit the organization-based information I share when using my personal device.	0.909			
PI4: I plan to limit the access applications have to organization-based information when using my personal device.	0.898			
PI5: I will likely enable private browsing when using my personal device.	0.836			
PI6: I will limit the ability of advertisers to track me when using my personal device.	0.763			
Perceived Severity [133, 134, 16]		0.915	0.933	0.701
PS1: If I break information security rules when using my personal device, my organization will discipline me.	0.862			
PS2: If I repeatedly break security rules when using my personal device, my organization will terminate me.	0.842			
PS3: If I were caught violating organization information security policies, I would be severely punished.	0.881			
PS4: I believe that organization information when stored on my personal device will be vulnerable to security incidents.	0.89			
PS5: I believe an organization's productivity and its employees will be threatened by security incidents when using a personal device.	0.791			
PS6: I believe the profitability of organizations is threatened by security incidents when using a personal device.	0.748			
Perceived Vulnerability [135, 23, 60]		0.88	0.909	0.625
PV1: I could be subjected to an information security threat if I don't comply with my own personal device security policy in my organization.	0.811			

PV2: If I don't comply with security policy when using my personal device, a security problem to my organization's information could occur.	0.772			
PV3: If I don't comply with the organization's security policy when using my personal device, a security problem to my personal data could occur.	0.791			
PV4: I know my organization could be vulnerable to security breaches if I don't adhere to it IS policy when using my personal device.	0.856			
PV5: I could fall victim to a malicious attack if I fail to comply with my organization's IS policy when using my personal device.	0.795			
PV6: If I don't pay adequate attention to guidelines when using my personal device, my organization's data and resources may be compromised.	0.71			
Response Cost [55, 23]		0.905	0.926	0.676
RC1: Complying with my personal device security policy interferes with my work.	0.874			
RC2: Complying with personal device security policy interferes with the personal use of my device.	0.805			
RC3: There are too many overheads associated with complying with personal device security policies.	0.782			
RC4: Complying with personal device security policy would require a considerable investment of effort other than time.	0.856			
RC5: Complying with personal device security policy would take a considerable amount of my working time.	0.843			
RC6: Complying with a personal device security policy would take a considerable amount of my personal time.	0.768			
Response Efficacy [55, 23]		0.893	0.92	0.699
RE1: Complying with my personal device security policy reduces the security threat to my organizations' information.	0.808			
RE2: Complying with my personal device security policy reduces the security threat to my personal data.	0.782			
RE3: If I comply with my personal device security policy, my organization's mobile security problems will be scarce.	0.861			
RE4: Compliance with my personal device security policy helps to reduce IS security problems in my organization.	0.885			
RE5: Compliance with my personal device security policy helps me reduce security problems with my own personal data.	0.838			
Subjective Norm [23; 51]		0.849	0.891	0.621
SN1: People who are influential to me think that I should follow the policies and procedures and use the security technologies for my personal device.	0.804			
SN2: I should follow the policies and procedures and use the security technologies for my personal device as people who are important to me think that.	0.754			
SN3: Top management thinks I should follow organizational IS security policies when using my personal device.	0.828			
SN4: My colleagues think that I should follow organizational IS security policies when using my personal device.	0.775			
SN5: I should follow organizational IS security policies when using my personal device as my organization's information security department thinks.	0.777			
Security Self-Efficacy [52, 54, 84]		0.858	0.892	0.623

SSE1: For me, taking information security precautions to protect my organization's information and information systems is easy when using my personal device.	0.718
SSE2: I have the expertise to protect my business and private data when using my personal device.	0.798
SSE3: I have the necessary skills to protect my organizations' information and information systems from information security violations when using my personal device.	0.823
SSE4: My skills required to stop information security violations against my organization's information and information systems are adequate when using my personal device.	0.786
SSE5: I believe that I could learn to perform preventive measures to protect my organization's information and information systems effectively when using my personal device.	0.816

Appendix B: Discriminant Validity

Constructs	ATT	ISA	KNOW	PB	PBC	PI	PS	PV	RC	RE	SN	SSE
ATT	**0.848**											
ISA	0.235	**0.781**										
KNOW	0.065	0.164	**0.817**									
PB	0.573	0.285	0.155	**0.846**								
PBC	0.549	0.152	0.127	0.545	**0.818**							
PI	0.423	0.257	0.26	0.65	0.451	**0.853**						
PS	0.499	0.327	0.15	0.707	0.484	0.541	**0.837**					
PV	0.471	0.355	0.266	0.516	0.353	0.438	0.365	**0.79**				
RC	0.342	0.218	0.033	0.459	0.289	0.364	0.401	0.268	**0.822**			
RE	0.433	0.19	0.109	0.499	0.357	0.368	0.429	0.475	0.26	**0.836**		
SN	0.407	0.487	0.218	0.517	0.414	0.442	0.47	0.36	0.191	0.382	**0.788**	
SSE	0.145	0.51	0.329	0.248	0.172	0.263	0.255	0.271	0.16	0.256	0.421	**0.789**