# Psychological Determinants of Cybersecurity Policy Compliance: A Case of Bangladeshi Undergraduate Students

**Abstract**

A significant number of students today conduct their lives using the internet and digital technologies. Due to their widespread use and capacity to store private and important data, these technologies and smart gadgets are a top target for hackers. However, there is still a serious problem with people's ignorance about IT security. Cyber security policies being disregarded has resulted in data leaks, reputational harm, and potential legal action. The integrated model given in this study is based on the General Deterrence Theory (GDT), Theory of Planned Behavior (TPB), and Protection Motivation Theory (PMT). The objective of this study is to discover the variables that affect students' compliance with online safety policies. This study creates and assesses a theoretical model of student behaviors to understand how students adhere to cyber security regulations. Finally, the theoretical model is tested empirically using data from a survey. The qualitative survey includes responses from 519 different students. This study only provided evidence for the general deterrence theory, which explains the heterogeneity in students' willingness to follow cyber security measures. The findings demonstrated that the Protection Motivation Theory and the Theory of Planned Behavior offer the strongest theoretical framework for explaining student behavior with relation to cyber security compliance.

**Keywords:** General Deterrence Theory, Theory of Planned Behavior, Protection Motivation Theory, Threat Appraisal, Security Policy Compliance, Coping Appraisal, Security Behavior.

**1. Introduction**

Cybersecurity issues are mostly occurring as a consequence of human error or negligence to security compliance act. It can be challenging to manage information security, especially when it comes to preventing threats from both insiders and outsiders. More precisely, there has been financial damage as a result of user noncompliance with privacy and security policies, laws, or procedures. People are the primary targets of malicious cyberattacks by cybercriminals (Saridakis et al., 2016). Worldwide technical development is resulting in an increase in IT security threats, which are also multiplying. In the current educational environment, the usage of IT-related resources is still need to be improved (Chingos et al., 2017; Sobaih & Elshaer, 2022). Making sure that the security precautions are in place to safeguard our personal information is essential.

The World Wide Web (WWW) is so broad and constantly changing that hackers take advantage of this (Safa et al., 2014). They breach security using numerous innovative ways. An example of a user error is using their Personal Identification Number (PIN) as their username and password, writing down their password in notebooks, sharing their login information with others, opening phishing emails, downloading files, and installing applications from the internet. The risk of cyber security attacks in the IT environment must therefore be reduced by implementing a number of security measures. Information system is at risk due to students' negligent security practices. The numerous and diverse issues that need to be addressed present a challenge for a single, standard framework.

The information system is endangered by students' irresponsible security procedures. The diverse and different security behaviors of IS security are difficult for a single, standard framework to handle (Nasir et al., 2019). The setting in which kids are exposed to their conduct can change (Wash & Rader, 2015). Students' behavior ought to be a major area of study for the IS security community. Student adherence to cyber security standards has been regarded as a crucial societal asset in light of the shift in emphasis from information security to human organizational views (Kirsch & Boss, 2007). To give students the best opportunity of coping with the behavioral difficulties related to information security management (ISM), to understand what drives them to behave in a way that complies with their cyber security regulations is significant.

One of the most notable research findings is that students at the university fail to comply with proposed legislation on data security (Reddy & Rao, 2016). When it comes to safeguarding personal emails or the university systems, faculty and students frequently disobey the best practices, placing their data in danger. Personnel working in higher education seem to perceive information security compliance as a safeguard against terrible events, such as the misuse of data, financial transactions, or private information, and as a result, they feel compelled to adhere to it (Sari et al., 2016).

To relieve end users' time and skill constraints, a number of security-related computational processes are being carried out automatically. Examples include patch management and virus updates. However, it's crucial to address matters like correct password usage, appropriate network resource consumption, and appropriate computer security requirements. Although the importance of reasonable computer use policies has long been emphasized, it is not yet clear what effects or efficacy these policies will have. The majority of the panelists who participated in ICIS 1993 stated that these restrictions are unnecessary despite the fact that they are necessary (Loch et al., 1998). There may still be compliance gaps even when the defined policies are explicit and thorough (Herath & Rao, 2009). In fact, if it makes their daily activities more convenient to do so, people may choose not to abide by security standards.

In this study, we looked at the factors affecting the cyber security practices of Bangladeshi undergraduate students. Through a review of the literature, a combined framework built on the GDT, TPB, and PMT is constructed in this paper. Thus, the students' intents to adhere to cyber security guidelines are assessed. This model was investigated using PLS-SEM in the SmartPLS 4.0.9.5 environment. To understand cyber security compliance policies more thoroughly, use our integrated model.

The remaining part of the paper is structured as follows:

* Section 2 presents the theoretical background for how to create an integrated model that is validated with empirical tests.
* Next, our hypotheses of the study are described in section 3.
* Section 4 contains the measures and methods of the research model along with the analysis of the data.
* Thereafter, section 5 presents the results of the study. Finally, we provide a discussion of our findings in section 6 and conclusion is given in section 7.

**2. Literature Review**

*2.1. Cybersecurity Behavior and Compliance with Cybersecurity Policies*

There are many psychological factors involved in cybersecurity behavior. Most scholars have employed the psychological theories of PMT, TPB, GDT, and many more intriguing ideas to examine cybersecurity behavior (Al-Omari et al., 2012; Boss et al., 2015). Compliance with security laws is the main subject of behavioral research on cybersecurity. The researchers discovered that behavioral issues prevented people from following cyber security policies, and they explore a number of elements that can assist make it easier for people to do so (Jones & Mitchell, 2016; Siponen et al., 2010). It also examined how cultural differences affect cyber security behavior because national cultures in each location have an impact on how they adhere to the rules (Connolly et al., 2019; Dinev et al., 2009). Numerous studies that examined the influence of protection motives on cyber security behavior discovered that people's perceptions of their own protection motivations have an impact on how successfully they adhere to privacy rules (Al-Omari et al., 2012; Lankton et al., 2019). It has been asserted that organizations with more robust cyber security cultures are less susceptible to cyberattacks (Lankton et al., 2019). Similar to this, when students are aware of cyber security, a positive safety culture is also created (Safa et al., 2015). Good tactics that promote the adoption of IT policies typically lead to the creation of a good cyber security environment (Hu et al., 2012).

*2.2. Protection Motivation Theory*

The idea of protection motive theory was put proposed by R.W. Rogers in 1975. It explains how people perceive risks and what steps they take to protect themselves in a health environment. The theory has been used widely to examine user IT security behavior in a variety of settings and in light of various risks. The theory aims to explain the idea of how protective actions start (Rogers, 1975). The coping appraisal and danger appraisal are the two essential ideas on which the PMT is based. Two categories make up the threat appraisal process: perceived severity and perceived vulnerability (Chenoweth et al., 2009). A person's sense of vulnerability in the face of a particular threat is referred to as their perceived vulnerability, and their perception of the threat's seriousness is referred to as their perceived severity. As part of the evaluation process, which is still divided into response efficacy, self-efficacy, and response cost (Chenoweth et al., 2009), a person's ability to take the proper steps to decrease the threat is assessed. The idea underlying self-efficacy is that users are capable of taking part in preventative measures. The effectiveness of the response is dependent upon confidence in the effectiveness of preventative measures. The costs related to using security measures are response costs. This threat assessment and coping assessment shapes the users' intentions to acquire protections.

*2.3. Theory of Planned Behavior*

A widely accepted social-psychological theory of human behavior is the Theory of Planned Behavior (Ajzen, 1991). TPB is a very popular theory of behavior and can be used to study the effects of beliefs on developing attitudes towards behavior, as well as their effect on behavioral intentions (Ajzen, 1991). TPB can be used to forecast particular actions in a variety of contexts, circumstances, and modes of action. Based on the TPB, three elements: perceived behavioral control, subjective norms, and attitudes together provide intentions to perform behaviors that lead to actual behavior (Ajzen, 1991). TPB specifically enables the prediction of certain behaviors across opportunities, circumstances, and varying types of acts. According to TPB, behavior is significantly influenced by intention (Beck & Ajzen, 1991).

The degree to which a person likes or dislikes something is related to their attitude toward that action. One's attitude toward conduct is influenced by the set of beliefs they have about a certain circumstance, a concept, a location, an activity, an object, or a person, which also influences their intention to behave in a particular way (Safa & Von Solms, 2016). Subjective norms serve as a representation for the outcomes of how a certain behavior is perceived (Safa & Von Solms, 2016). The term perceived behavioral control (PBC) refers to how difficult an activity is perceived to be for a person to carry out (Ajzen, 1985). PBC, then, is the capacity of an individual to engage in a particular activity (Ajzen, 1985). PBC is based on the controllability and usability notions in an effort to anticipate security protection intents (Qing & Dinev, 2005).  
Subjective norms are crucial for ensuring security awareness (Banerjee et al., 1998), and they also affect intents and actions related to information system security policy (ISSP) compliance (Ifinedo, 2014). The knowledge of security issues may affect users' attitudes and behavior (Dinev & Hu, 2007). In the IT sector, one of the most crucial factors in shaping attitudes is user awareness of vulnerabilities (Dinev & Hu, 2007).

*2.4. General Deterrence Theory*

To understand the impacts of deterrent elements with respect to security laws, general deterrence theory from criminology is applied. The theory of general deterrence was established from criminology. It suggests that people are discouraged from engaging in certain behavior as a result of harsh, quick, and certain sanctions (Abramovaite et al., 2022). Deterrence is also seen as a useful mechanism for governance, with evidence that it helps to reduce undesirable behavior. The severity of sanctions or penalties may have a serious effect on the motivations of ISPs to follow these policies, but the correlation between their compliance and these policies is positive. Table 1 highlights different techniques used in determining security intentions.

**Table 1** Summary of the related studies

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sl. | Author and Year | Theory | Dependent variables | Independent variables | Sample size &  Respondents | Method | Analysis technique | Findings |
| 1. | (Ifinedo, 2012) | TPB, PMT | ISSP intention | Perceived severity,  Subjective norms, Response cost, Perceived vulnerability, Self-efficacy,  Attitude,  Response efficacy | 124  business managers  and  IS  professionals | Questionnaire survey | Partial  least  squares  (PLS) technique. | ISSP was affected by perceived vulnerability, response efficacy, self-efficacy, and attitude |
| 2. | (Siponen et al., 2014) | Theory of Reasoned Action Cognitive Evaluation Theory, PMT | Intention to comply with ISP,  Actual compliance with ISP | Normative beliefs, Response efficacy, Rewards,  Self-efficacy  Severity, Attitude,  Vulnerability | 669 employees | Self-reported questionnaire | AMOS 6.0 SEM software and SPSS 14.0 | Beliefs, perceived severity, self-efficacy, attitude, and vulnerability all had a major impact on the intention to follow IS regulations, while rewards and response efficacy had no effect |
| 3. | (Thompson et al., 2017) | PMT,  psychologi-cal ownership, and Social influence | Personal computing security intentions | Descriptive norm, Perceived severity, Response efficacy, Prior experience, Subjective norm, Perceived vulnerability, Response cost, Self-efficacy | 629 mobile device users and home computer | Questionnaire | PLS technique | Descriptive norm, self-efficacy, psychological ownership, response cost, and perceived vulnerability all influenced behavior and PCSI, but neither subjective norm nor response efficacy had an impact on security intentions |
| 4. | (Farooq, Jeske, et al., 2019) | IMB Model | Security Behavior | Measures Familiarity, Social Support Threat Awareness, Security Attitude,  Self-efficacy | 159 university students | Two-part online survey | PLS-SEM 3.2 | The IMB was a suitable model for the analysis and prediction of students security behavior |
| 5. | (Ernovianti et al., 2012) | TAM | Behavioral intention | Self-efficacy, Usefulness, Credibility,  Ease of use,  Compatibility | 170 students | Questionnaire  survey | Structural equation modeling (SEM) using AMOS 18 | Self-efficacy estimates internet banking intention |
| 6. | (Verkijika, 2018) | Anticipated regret, PMT | Security intention,  Security Behavior | Response cost,  Self-efficacy, Response efficacy, Perceived vulnerability, Anticipated regret, Perceived severity | 385 smartphone device owners | Questionnaire survey | SmartPLS 3.0 | Self-efficacy significantly correlated with intentions to secure smartphones, while perceived severity and perceived vulnerability significantly influenced anticipated regret |
| 7. | (Hanus & Wu, 2016) | PMT | Security Behavior | Awareness, Response cost, Perceived vulnerability, Self-efficacy, Perceived severity, Response efficacy | 241  university  students | Questionnaire  survey | SmartPLS software | The coping appraisal process with the exception of response cost, significantly impacts security behavior, and security behavior is highly impacted by security awareness, which also has a considerable impact on self-efficacy, perceived severity, response cost, and response efficacy |
| 8. | (Koohang et al., 2021) | UMISPC | Reactance,  Intention | Fear, threat, Response-efficacy, Role values, Habit,  Neutralization | 187 faculty and staff | Survey | SmartPLS 3.0 | The proposed model was strong, valid, and reliable |
| 9. | (Vance et al., 2012) | Habit Theory, PMT | ISPCI | Response cost, Perceived severity, Self-efficacy,  Habit, Response efficacy, Vulnerability, Rewards | 210 IS managers and IS security experts | Questionnaire  Survey | SmartPLS 2.0 | Employee intention for future compliance was highly reinforced by HISC which also supported the theories suggested by PMT |
| 10. | (Al-Omari et al., 2012) | TPB | ISPCI | Subjective norm, Attitude, Self-efficacy, Awareness | 878 employees | Questionnaire  survey | SmartPLS | Users attitudes and behaviors will change to become more security-conscious as a result of establishing a culture within the organization that values security |
| 11. | (Safa et al., 2015) | PMT, TPB | ISCCB | Threat appraisal, IS awareness, Attitude, Organizational policies, Information security, Subjective norms, Experience and involvement, self-efficacy, Perceived behavioral control | 212 IT  Professionals and IS Experts | Questionnaire  Survey | PLS-SEM and IBM AMOS 20 | User behavior was influenced by attitude, IS organisation policy, awareness of IS, involvement in IS, subjective norms, information security, self-efficacy, and threat assessment. The perception of behavioral control, however, has minimal effect on security behavior |
| 12. | (Safa & Von Solms, 2016) | Triandis model, TPB, Motivation Theory | ISKS behavior,  ISKS intention | Trust, Attitude, Extrinsic motivation, Perceived behavioral control Subjective norms, Intrinsic motivation, Organizational support | 482 employees | Questionnaire  Survey | SEM using IBM AMOS 20 | Perceived behavioral control, subjective norms, and attitude had a favourable influence on information security knowledge sharing intention, and ISKS intention affects ISKS behavior |

**3. Hypothesis formulation and model development**

*3.1.* *Relationship between PMT and security policy compliance intention*

In order to analyze user intentions and behaviors towards security in both professional and home-use contexts, a theoretical framework based on PMT has been utilized (Ifinedo, 2012; Lee et al., 2017; Vance et al., 2012). PMT helps to understand the threats and their effectiveness in coping with them, which can provide a basis for individual views as to whether or not security policies are necessary. A person can learn about cyber security concerns and develop a general understanding of them in terms of the security of data via a range of sources, including conversations inside the organization, online communities, and external media. The cognitive assessment of two processes gives rise to PMT: coping appraisal and threat appraisal. Threat appraisal takes into account the perception that a person feels threatened, based on an assessment of the factors influencing the appeal of fear (Herath & Rao, 2009). Perceived severity (the level of impact related to the attack) and perceived vulnerability (the chance that the danger would appear) are the PMT indicators that reflect threat appraisal. Both for home users and for organizations, perceived severity and vulnerability are important predictors of protective intentions (Ifinedo, 2012; Lee et al., 2017; Vance et al., 2012). Students tend to be concerned if they think an attack on security could cause serious harm or disruptions. In summary, people are more inclined to perceive measures to prevent attacks, such as security rules, when they think the threat is severe and are worried about it. Table 2 represents the main theories and related constructs.

**Table 2** Number of constructs and related theories

|  |  |
| --- | --- |
| **Constructs** | **Theory** |
| Perceived vulnerability | PNG |
| Security breach concern level |
| Perceived severity |
| Self-efficacy |
| Response cost |
| Response efficacy |
| Security policy attitude | TPB |
| Descriptive norm |
| Awareness |
| Subjective norm |
| Detection certainty | GDT |
| Punishment severity |

The following hypotheses are put forth to investigate the relationship between perceived vulnerability and perceived severity and the security goals of university students in response to the conflicting findings and the consideration of the PMT model. We can therefore hypothesize:

**H1:** *Perceived vulnerability will positively affect students level of security breach concern.*

**H2:** *Perceived severity* *will positively affect the students level of security breach concern.*

The second PMT technique that is crucial for preserving attitudes is the coping appraisal. Self-efficacy, response costs, and response effectiveness are some of its markers. In addition to financial costs, response costs also take into account the time, effort, and challenges that users had to face as a result of their security-related activities (Lee et al., 2017). According to Lee et al. (2017), response costs had a detrimental impact on protective motivation. The inconvenience that security measures entail is one of the reasons why students dislike or ignore them in the domain of IS. Response costs and behavioral intention have a negative association, according to study findings on students' security behaviors (Lee et al., 2017). Therefore, we determine the given hypothesis:

**H3:** *Response costs will negatively affect students security policy compliance intentions.*

Self efficacy describes how a person feels about their capacity to complete a particular activity. Despite the fact that self-efficacy is considered a key component of protective motivation, TPB also heavily relies on it (Herath & Rao, 2009). In recent studies, security intention was significantly influenced by response efficacy and self-efficacy in both business and home-user environments (Ifinedo, 2012; Lee et al., 2017; Marikyan et al., 2022). Regarding the association between student behavior intentions, response efficacy, and self-efficacy, we put forth the following hypotheses:

**H4:** *Self efficacy will positively affect students security policy compliance intentions.*

**H5:** *Response efficacy will positively affect students security policy compliance intentions.*

The study presented here defines security concern as the level at which students believe their personal information are in danger. It is likely that students will be more concerned if they believe that a security threat can cause significant damage or disturbance. Thus, we can hypothesis:

**H6:** *Security breach concern level will positively affect the security policy compliance intention of students.*

*3.2.* *The link between theory of planned behavior and security policy compliance intention*

In the literature on IS, numerous studies have examined the connection between behavioral intentions and attitudes (Alyoussef, 2022). In most research, the connection between attitude and behavior intentions is discussed in the context of an organization. The positive correlation between attitudes towards security and behavioral intentions has been shown in several studies (Bulgurcu et al., 2010; Ifinedo, 2012; Lee et al., 2017). To understand more about how students security intentions and attitudes are related, the following hypothesis was tested:

**H7:** *The security policy attitude will have a positive effect on students security policy compliance intentions.*

The subjective norms are the TPB construct. In order to create a classroom environment where students abide by security requirements, social influence is crucial (Ifinedo, 2012). The analysis of social influence makes use of subject norms. Social effect is the extent to which social networks influence behavior by disseminating knowledge and guidelines that help people understand the significance of a particular task (Venkatesh et al., 2001). The social effects of exercising security-related precautions when using personal computers at home and the internet have been studied using subjective and descriptive norms (Anderson & Agarwal, 2010). Subjective norms have a significant impact on how safety protocols for home computer systems are applied. Subjective norms are developed based on reasons for compliance and normative beliefs. According to Rivis and Sheeran (2003) and Sheeran & Orbell (1999), the main goal of descriptive norms is to determine how much a person believes that other people behave in a certain way or their propensity to copy others' behavior. According to a study (Vance et al., 2012), descriptive norms are significantly influenced by security intentions. To examine the essence of students security intentions, these given hypotheses are presented:

**H8:** *Subjective norms will positively affect the security policy compliance intention of students.*

**H9:** *Descriptive norms will positively affect the security policy compliance intention of students.*

The core components of IS are awareness and conduct. In order to avoid victimization, users must be aware of social technologies (Straub, 1990). According to Marikyan et al. (2022) IS awareness is seen as an essential element of IS behavior. According to Bulgurcu et al. (2010) and Rocha Flores & Ekstedt (2016), IS awareness is also described as a basic idea and comprehension of information security policy (ISA). Collaboration, intervention, and the dissemination of knowledge about information security all have an impact on how people view and feel about information security (Feledi et al., 2013; Tamjidyamcholo et al., 2014). According to Tamjidyamcholo et al. (2014), the study showed a link between attitudes about security and compliance with intentions. Therefore, the following hypothesis is suggested:

**H10:** *Awareness is positively associated with the security policy attitude.*

*3.3. General deterrence theory-related hypotheses*

According to the deterrence theory, the level of inappropriate behavior declines as punishment severity and detection certainty. Essentially, there is a possibility of stopping undesirable behavior by means of an immediate or serious penalty (Akers, 1973; Williams & Hawkins, 1986). In the case of organizational software piracy, punishment severity strongly influenced attitudes toward piracy (Peace et al., 2003). If people perceive that there will be serious consequences for breaking the rules, they are less likely to participate in the undesirable behavior. Therefore, we expect the following hypothesis:

**H11:** *Punishment severity will positively affect the security policy compliance intention of students.*

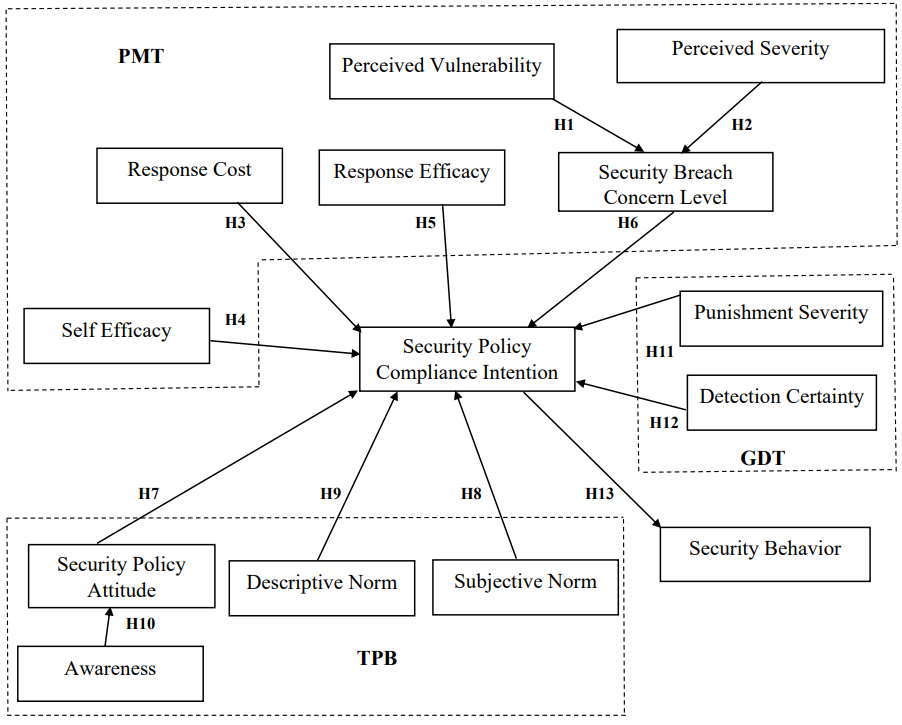
The certainty and seriousness of organizational action are both taken into account during enforcement. According to deterrence theory, if potential offenders are aware that measures are being taken to combat antisocial conduct, they will be discouraged from undesirable acts by a harsh and certain punishment. Assuming potential offenders are aware of efforts to combat antisocial conduct, the deterrence theory states that harsh and certain sanctions will dissuade them from engaging in undesirable acts (Peace et al., 2003; Straub, 1990). According to the statement that "preventive efforts significantly affect the amount of security for data criminals due to the extent of these attempts relative to the certainty of punishment," businesses can employ both tactics and technology to monitor right actions (Kankanhalli et al., 2003). Hence, we hypothesize:

**H12:** *Detection certainty will positively affect the* *security policy compliance intention of students.*

*3.4. Security policy compliance intention and security behavior*

The intention-based model has been used in most security studies where PMT and TPB have been used. The idea that behavior genuinely reflects intention is supported by research, even though it is debatable whether security behavior actually results from security intention (Egelman et al., 2016). To show that intention is more capable of influencing actual behavior to conform with policies, a study on organisational practices was undertaken (Siponen et al., 2014). The research model for this study is displayed in Figure 1. The following hypothesis has been presented to assess whether security intentions predict the behavior of students:

**H13:** *Security policy compliance intention will positively affect the* *security behavior of students.*



**Figure 1.** Reaearch Model

**4. Research Methodology**

*4.1. Research Model*

The proposed model combines the PMT theory, the TPB theory, the GDT theory, and a new construct for security behavior. Security behavior is a formative construct, and it is a variable that depends on others (Chin, 1998). All theory-related constructs remained reflective, with the exception of security behavior. Constructs are collections of variables that depict a common variance through several factors, whereas reflective constructs are combinations of variables that demonstrate a common factor when the factor shifts from construct to item (Chin, 1998). In order to conduct an empirical test of the relationships proposed by the research model, data were collected using a survey technique. The techniques for developing instruments and managing surveys are covered in detail in the following sections.

*4.2. Questionnaire Development and Procedure*

The information was acquired by means of an online survey that was written in English and used Google Forms as its online survey tool. Two sections of the questionnaire were used: one to collect background and demographic data on the participants, and the other to identify the variables that influence undergraduate Bangladeshi students' adherence to cyber security policies. A total of 65 questionnaires were created for the purpose of this research. Male and female university students were each given a link to a Google form that was used to gather information.

*4.3. Instrument Development*

The study includes fourteen constructs, namely, Awareness (4 items), Security Policy Attitude (6 items), Descriptive Norm (3 items), Perceived Severity (5 items), Security Policy Compliance Intention (6 items), Response Efficacy (3 items), Perceived Vulnerability(6 items), Security Breach Concern Level (2 items), Response Cost (5 items), Security Behavior (4 items), Punishment Severity (2 items), Self-Efficacy (8 items), Subjective Norm (4 items), and Detection Certainty(2 items). We used the items from earlier validated research with some linguistic alterations to fit in the framework of cyber security policy compliance intentions in order to reduce issues with the questionnaire's validity and accuracy. A 5-point Likert scale is used in each item to show the degree of agreement with comments about the likelihood that a responder is following the intentions. A 5-point Likert scale was used to estimate the respondents' level of agreement, with 1 denoting a strong disagreement and 5 denoting a strong agreement. The number of items for each construct as well as the origin of each construct's components used in this study are shown in Table 3.

**T****able 3**  Details of Construct with Sources

|  |  |  |  |
| --- | --- | --- | --- |
| Construct | Sample Item | | Source |
| Perceived Vulnerability | PV1 | I might be the target of a major data security threat. | (Ifinedo, 2012; Siponen et al., 2014; Thompson et al., 2017; Woon et al., 2005) |
|  | PV2 | I'm in danger if my password is weak. | (Siponen et al., 2014) |
|  | PV3 | If my password is weak, it is hazardous when I use my account. | (Woon et al., 2005) |
|  | PV4 | I believe that a security threat could affect my smartphone. | (Thompson et al., 2017; Verkijika, 2018) |
|  | PV5 | If I don't use excellent smartphone security practices, I might become the victim of a threatening attack. | (Thompson et al., 2017; Verkijika, 2018) |
|  | PV6 | I run the danger of getting a virus on my equipment. | (Hanus & Wu, 2016) |
| Perceived Severity | PSS1 | This would be a major problem for me if there was a security attack on my system or account. | (Ifinedo, 2012; Siponen et al., 2014; Woon et al., 2005; Workman et al., 2008) |
|  | PSS2 | There will be serious repercussions if my passwords and personal information are revealed. | (Woon et al., 2005; Workman et al., 2008) |
|  | PSS3 | My account is seriously at risk if my password becomes known by another person. | (Workman et al., 2008) |
|  | PSS4 | If my password had been hacked, I might suffer significant losses. | (Siponen et al., 2014) |
|  | PSS5 | I think it's a major concern when my computer becomes infected with a virus. | (Hanus & Wu, 2016) |
| Response Cost | RC1 | Implementing security measures would be time-consuming. | (Thompson & Mcgill, 2017; Woon et al., 2005; Workman et al., 2008) |
|  | RC2 | It is difficult to adopt security technologies and practices. | (Thompson & Mcgill, 2017) |
|  | RC3 | Installing security features on my phone would be a big hassle. | (Thompson et al., 2017; Verkijika, 2018) |
|  | RC4 | The benefits of installing the suggested security precautions on my phone exceed the costs. | (Thompson et al., 2017; Verkijika, 2018) |
|  | RC5 | Updating my operating system will be quite expensive. | (Hanus & Wu, 2016) |
| Response Efficacy | RE1 | Enabling security measures will prevent security breaches. | (Woon et al., 2005; Workman et al., 2008) |
|  | RE2 | The best way to avoid hackers is to implement protective measures on my phone. | (Thompson et al., 2017; Verkijika, 2018) |
|  | RE3 | The protective measures used to prevent unauthorized access to my smartphone’s private data, including financial information, are effective. | (Verkijika, 2018) |
| Self Efficacy | SE1 | I'm comfortable taking preventative actions to protect data. | (Anderson & Agarwal, 2010; Woon et al., 2005) |
|  | SE2 | Without much effort, I'm capable of changing my password. | (Anderson & Agarwal, 2010) |
|  | SE3 | It's easy for me to learn how to change the password. | (Anderson & Agarwal, 2010; Woon et al., 2005) |
|  | SE4 | I'm familiar with how to change my password. | (Chiesi et al., 2020) |
|  | SE5 | If I want, I can follow the security procedures myself. | (Chiesi et al., 2020; Tangney et al., 2018) |
|  | SE6 | Even if there were no one there to help me, I could still follow to most of security rules. | (Woon et al., 2005) |
|  | SE7 | I have to stop doing stuff that's bad for me and others on social media. | (Chiesi et al., 2020; Tangney et al., 2018) |
|  | SE8 | I'm comfortable taking precautions to keep my phone safe. | (Thompson et al., 2017; Verkijika, 2018) |
| Security Policy Attitude | SPA1 | To protect my information, I will take security precautions. | (Farooq, Jeske, et al., 2019; Taylor & Todd, 1995) |
|  | SPA2 | The mandatory password update will make using my account safer. | (Taylor & Todd, 1995) |
|  | SPA3 | I'm in favor of a process that requires my password to be changed. | (Ernovianti et al., 2012) |
|  | SPA4 | It is important to adopt security technologies and practices. | (Farooq, Jeske, et al., 2019; Taylor & Todd, 1995) |
|  | SPA5 | It's beneficial to adopt security technology and practices. | (Farooq, Jeske, et al., 2019; Taylor & Todd, 1995) |
|  | SPA6 | Avoiding problematic social media use will help me use the internet more effectively. | (Yakubova et al., 2015) |
| Subjective Norm | SN1 | Those who are significant to me have advised me to take care to secure my information. | (Ernovianti et al., 2012; Taylor & Todd, 1995) |
|  | SN2 | My classmates may think it's a good idea for me to modify my PID (Personal Identification) password. | (Taylor & Todd, 1995) |
|  | SN3 | My PID (Personal Identification) password should be changed, according to those who have influence of my decisions. | (Ernovianti et al., 2012; Taylor & Todd, 1995) |
|  | SN4 | I should update my password, according to people who are important to me. | (Yakubova et al., 2015) |
| Descriptive Norm | DN1 | I believe that other people use protection measures. | (Anderson & Agarwal, 2010; Ernovianti et al., 2012) |
|  | DN2 | I'm sure everyone is following the security policy of the institution. | (Herath & Rao, 2009) |
|  | DN3 | Most organizations are expected to follow security policies to protect internal security. | (Herath & Rao, 2009) |
| Security Policy Compliance Intention | SPCI1 | I'm going to take steps to secure my information. | (Taylor & Todd, 1995; Woon et al., 2005) |
|  | SPCI2 | I might make some kind of security measures to keep my phone safe. | (Thompson et al., 2017; Verkijika, 2018) |
|  | SPCI3 | I believe that I will stop before clicking on links from sources that are not reliable. | (Witte et al., 1996) |
|  | SPCI4 | I will think twice before buying essentials from unknown websites. | (Witte et al., 1996) |
|  | SPCI5 | In accordance with the internet service provider, I want to secure information and technological resources. | (Koohang et al., 2021) |
|  | SPCI6 | I'm ready to abide by the ISP in the future. | (Sohrabi Safa et al., 2016) |
| Awareness | AW1 | I understand the conditions for changing my password. | (Melović et al., 2020) |
|  | AW2 | I understand the rules and requirements needed to update my password. | (Taylor & Todd, 1995) |
|  | AW3 | I know it is my responsibility to change my password. | (Melović et al., 2020) |
|  | AW4 | To increase public understanding of internet abuse and its consequences, I must keep working. | (Melović et al., 2020) |
| Detection Certainty | DC1 | For policy violations, students computer practices are properly monitored. | (Ketchen, 2013) |
|  | DC2 | I'm likely to be arrested if I break any security rules. | (Ketchen, 2013) |
| Punishment Severity | PS1 | If I’m found to be breaking the policy concerning information security at my educational institutions, I would get a severe penalty. | (Herath & Rao, 2009) |
|  | PS2 | Students who persistently disobey security policies are dismissed from my institution. | (Herath & Rao, 2009) |
| Security Breach Concern Level | SBCL1 | The threat to Information Security is excessive. | (Herath & Rao, 2009) |
|  | SBCL2 | Information Security is important, and we need to keep an eye on it. | (Herath & Rao, 2009) |
| Security Behavior | SB1 | I use different passwords for different accounts. | (Farooq, Jeske, et al., 2019) |
|  | SB2 | I want to teach friends effective internet usage techniques. | (Jones & Mitchell, 2016; Saputra et al., 2021) |
|  | SB3 | On my personal devices, I regularly use antivirus and antimalware software. | (Verkijika, 2018) |
|  | SB4 | To keep my personal device safe from threats, I regularly update my operating system. | (Hanus & Wu, 2016) |

Along with the information mentioned above, the questionnaire also captured demographic data about the respondents, including their gender, age, education level, hometown, and the social media platforms they mainly use to access the internet.

*4.4. Data Collection and Sampling frame*

The study's actual respondents were Bangladeshi undergraduate students currently enrolled. The survey was accompanied by a cover sheet outlining the main goal of the study. It also included the consent form informing respondents of their right to privacy and a statement of their decision not to participate. Items for the following subscales were distributed to participants: Awareness, Self-Efficacy, Security Policy Attitude, Descriptive Norm, Perceived Vulnerability, Response Cost, Perceived Severity, Security Policy Compliance Intention, Detection Certainty, Response Efficacy, Security Behavior, Security Breach Concern Level, Subjective Norm, and Punishment Severity. Table 4 also included the items pertaining to demographic information. The data was gathered between June 15 and June 25, 2023. In order to accomplish this, 519 replies were compiled, all of which met the requirements for attention-checking. Participants ranged in age from 18 to 32, had some education, and resided in both urban and rural locations.

*4.5. Method for Data Analysis*

The research was conducted using the Partial Least Squares Structural Equation Modelling (PLS-SEM) technique, which is developing as an essential statistical modeling technique, and was used for analysis (Koohang et al., 2021). We used SmartPLS 4.0.9.5 environment for data analysis. In studies on information security, PLS is used to a large extent. The PLS-SEM process is divided into two steps: first, the measurement model is tested (reliability and validity), and second, the structural model is tested (hypothesized relationship test). Furthermore, to assess the loadings and path coefficient significance, bootstrapping method of 5000 resamples was used (Koohang et al., 2021).

**5 Results**

*5.1. Profiles of Respondents*

Table 4 illustrates the respondents profiles. There were 269 males (51.8%) and 250 females (48.2%). Majority of the respondents (387) were between 18 to 25 years old, 88 were 25-30 years old and only 44 were 31 years old and above. It was also found that the number of undergraduate student’s percentage was high (74.4%) whereas the number of diploma student’s percentage was significantly low (25.6%). On the basis of residence, 70.3% of the respondents lived in urban areas. The highest percentage of respondents were Facebook users (32.4%), followed by a decreasing percentage of Messenger users (21.8%), Instagram users (20.8%), WhatsApp users (11.8%), and finally YouTube users (13.3%) respectively.

**Table 4** Demographic characteristics of the respondents

|  |  |  |  |
| --- | --- | --- | --- |
| **Characteristics** | **Type** | **Frequency** | **Percent (%)** |
| Gender | Male | 269 | 51.8 |
| Female | 250 | 48.2 |
| Age (years) | 18-25 years | 387 | 74.6 |
| 25-30 years | 88 | 17 |
| 31 and above | 44 | 8.5 |
| Education | Bachelor | 386 | 74.4 |
| Diploma | 133 | 25.6 |
| Hometown | Rural | 154 | 29.7 |
| Urban | 365 | 70.3 |
| Mostly used Social Media | Facebook | 168 | 32.4 |
| Messenger | 113 | 21.8 |
| Instagram | 108 | 20.8 |
| WhatsApp | 61 | 11.8 |
| YouTube | 69 | 13.3 |

*5.2.* *Measurement Model*

Prior to looking at the structural model, it was necessary to test the validity and reliability of the latent variables with the intention of examining the provided hypotheses. The following steps were performed in order to test the measurement model:

* Step 1: To assess the reliability of the research model, the preceding criteria were used: Table 5 presents the results for factor loadings, Composite Reliability (CR), Cronbach's alpha, and Average Variance Extracted (AVE). Factor loading should be at least equal to or greater than 0.70 (Hair et al., 2014). The analysis removed indicators with loadings below 0.70. These indicators, PV6 (0.360), RC4 (0.157), SB3, and SB4 (0.154 and 0.086), SE1, SE2, and SE4 (0.255, 0.369, and 0.155), SN2 (0.399), PS2 (0.440), and DC2 (0.360), were removed, respectively, as they contain the value of factor loadings < 0.70. Indicator reliability was obtained after these were removed from the dataset, the data were reanalyzed, and these were eliminated. Factor loading of 0.70 or more is preferable, while 0.4 or higher is acceptable if the study is exploratory (Purwanto & Sudargini, 2021). A minimum factor loading of 0.6 was stipulated (Hair et al., 2014). The composite reliability (CR) and Cronbach's alpha (α) tests were used to evaluate the reliability of internal consistency. The cutoff value for each was ≥ 0.70 (Hair et al., 2019). All latent variables in Table 5 met this requirement
* Step 2: The following criteria were used to assess the validity of the research model: For divergent validity and convergent validity, the Average Variance Extracted (AVE) criterion is ≥ 0.50 (Fornell & Larcker, 1981; Koohang et al., 2021). The AVE for each item was higher than this cutoff point, illustrating convergent validity and divergent validity. All values were provided in Table 5.
* Step 3: Furthermore, the findings of the lateral collinearity assessment among the variables are shown in Table 5. For the interconstruct, the Variance Inflation Factor (VIF) should be < 5 (Kock, 2015). Table 5 displays the findings of the inner (VIF) values for the exogenous variables (i.e., Descriptive Norm, Response Efficacy, Perceived Severity, Awareness, Security Behavior, Perceived Vulnerability, Response Cost, Security Breach Concern Level, Self-Efficacy, Security Policy Compliance Intention, Subjective Norm, Detection Certainty, Security Policy Attitude, and Punishment Severity). All the values in Table 5 were less than the value of '5', which is the minimum accepted value. This proves that, there is no multicollinearity problem in the model.

*5.2.1 Heterotrait-Monotrait (HTMT) ratio, cross-loading, and the Fornell-Larcker criterion*

Heterotrait-Monotrait (HTMT) ratio, cross-loading, and the Fornell-Larcker criterion are three techniques used to measure discriminant validity. Discriminant validity indicates how different each construct from the others.

**Fornell-Larcker criterion** (Fornell & Larcker, 1981; Koohang et al., 2021) provides a quantitative assessment of discriminant validity by comparing the shared variance captured by a construct (AVE) with the squared correlations between constructs. It helps ensure that constructs are distinct and not measuring the same underlying latent variable. Mathematically, the Fornell-Larcker criterion is expressed as:

The Fornell-Larcker criterion states that for a construct to have discriminant validity, its AVE should be greater than the squared correlations (correlations between constructs) with all other constructs in the model, suggests that the construct has adequate discriminant validity.

In Table 6, the correlation matrix for the Fornell-Larcker criterion, the square root of the AVE for each latent variable in this study was greater than its maximum correlation with any other latent variable (Fornell & Larcker, 1981). Thus, the measuring model appears to be satisfactory on the basis of the reliability and validity evaluation.

**Cross-loading** (J Henseler, et al. 2015) in the context of discriminant validity refers to a situation where an item from a measurement scale (e.g., a questionnaire) loads significantly on more than one underlying construct or factor. Cross-loadings is to examine the standardized factor loadings in a measurement model can be expressed as:

Where, Covariance (j,F) is the covariance between the indicator (j) and the latent construct (F).

In the presence of cross-loadings, you might observe high factor loadings for an item on multiple constructs. This suggests that the item is not uniquely measuring one specific construct, which can lead to a lack of discriminant validity. Addressing cross-loadings is important for ensuring that measurement model accurately reflects the underlying theoretical constructs. Cross-loading results are used to assess another criterion for discriminant validity. When cross-loading techniques are used, the outcome appears to be reliable. Each indicator had high loading factors according to their construct, as shown in Table 5. Therefore, there was no problem with high cross-loading between them.

**Heterotrait-Monotrait Ratio of Correlations (HTMT) (**Ab Hamid, et al. 2017) is a measure used to assess discriminant validity in structural equation modeling (SEM). Heterotrait Correlations refer to correlations between different constructs. Monotrait Correlations refer to correlations within the same construct. The HTMT is calculated as follows:

The heterotrait-monotrait (HTMT) ratio showed for all items in Table 7. HTMT values < 0.85 produce the best outcomes (Rasoolimanesh, 2022). All values in Table 7 met the criteria and indicated the establishment of discriminant validity. The correlation between two latent variables is estimated using HTMT. This index is used to make up for the lack of sensitivity by demonstrating the discriminant validity of the cross-loading methods and Fornell-Larcker criterion. These findings led to a decision that the model was reliable, internally consistent, and had enough discriminant validity.

**Table 5** Results of Measurement assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Construct | Item | Mean | SD | Loadings | Cronbach’s  α ≥ 0.70 | AVE≥ 0.50 | CR ≥ 0.70 | VIF |
| **Awareness** | AW1 | 5.022 | 1.440 | 0.963 | 0.942 | 0.803 | 0.947 | 2.112 |
| AW2 | 5.100 | 1.043 | 0.929 | 2.390 |
| AW3 | 5.001 | 1.028 | 0.906 | 2.011 |
| AW4 | 4.107 | 1.001 | 0.775 | 2.032 |
| **Descriptive Norm** | DN1 | 4.655 | 1.201 | 0.903 | 0.894 | 0.734 | 0.910 | 1.037 |
| DN2 | 4.435 | 1.230 | 0.690 | 1.023 |
| DN3 | 4.699 | 1.405 | 0.954 | 2.008 |
| **Perceived Severity** | PSS1 | 4.321 | 1.231 | 0.809 | 0.900 | 0.645 | 0.912 | 2.034 |
| PSS2 | 4.282 | 1.204 | 0.624 | 1.034 |
| PSS3 | 4.711 | 1.490 | 0.855 | 2.074 |
| PSS4 | 4.745 | 1.193 | 0.946 | 2.610 |
| PSS5 | 4.001 | 1.105 | 0.745 | 2.146 |
| **Perceived** **Vulnerability** | PV1 | 4.868 | 1.304 | 0.945 | 0.964 | 0.841 | 0.968 | 2.013 |
| PV2 | 4.645 | 1.802 | 0.983 | 2014 |
| PV3 | 4.585 | 1.421 | 0.980 | 2.002 |
| PV4 | 4.894 | 1.601 | 0.863 | 1.021 |
| PV5 | 4.225 | 1.300 | 0.800 | 1.410 |
| **Response Cost** | RC1 | 5.021 | 1.001 | 0.940 | 0.972 | 0.895 | 0.972 | 1.310 |
| RC2 | 4.011 | 1.360 | 0.919 | 1.040 |
| RC3 | 4.589 | 1.412 | 0.962 | 1.343 |
| RC5 | 4.565 | 1.327 | 0.963 | 2.000 |
| **Response Efficacy** | RE1 | 4.555 | 1.741 | 0.891 | 0.958 | 0.887 | 0.961 | 3.000 |
| RE2 | 5.033 | 1.274 | 0.991 | 2.327 |
| RE3 | 5.021 | 1.366 | 0.940 | 2.017 |
| **Security** **Behavior** | SB1 | 3.069 | 1.251 | 0.778 | 0.700 | 0.542 | 0.706 | 1.027 |
| SB2 | 3.022 | 1.371 | 0.691 | 1.043 |
| **Security Breach Concern Level** | SBCL1 | 4.193 | 1.241 | 0.960 | 0.962 | 0.927 | 0.962 | 2.022 |
| SBCL2 | 4.308 | 1.258 | 0.966 | 2.703 |
| **Self-Efficacy** | SE3 | 45.230 | 1.364 | 0.955 | 0.951 | 0.793 | 0.954 | 1.250 |
| SE5 | 3.069 | 1.300 | 0.767 | 1.425 |
| SE6 | 4.403 | 1.253 | 0.909 | 1.273 |
| SE7 | 4.047 | 1.302 | 0.921 | 1.003 |
| SE8 | 4.003 | 1.163 | 0.890 | 1.381 |
| **Subjective Norm** | SN1 | 4.013 | 1.242 | 0.823 | 0.942 | 0.851 | 0.951 | 2.012 |
| SN3 | 4.958 | 1.004 | 0.965 | 2.520 |
| SN4 | 4.654 | 1.041 | 0.971 | 2.610 |
| **Security Policy Attitude** | SPA1 | 4.327 | 1.064 | 0.868 | 0.968 | 0.835 | 0.969 | 1.049 |
| SPA2 | 4.713 | 1.333 | 0.945 | 1.572 |
| SPA3 | 4.666 | 1.485 | 0.936 | 1.379 |
| SPA4 | 4.005 | 1.317 | 0.923 | 1.725 |
| SPA5 | 3.890 | 1.107 | 0.868 | 1.247 |
| SPA6 | 4.820 | 1.322 | 0.940 | 1.364 |
| **Security Policy Compliance Intention** | SBCI1 | 4.120 | 1.073 | 0.878 | 0.963 | 0.811 | 0.963 | 2.043 |
| SBCI2 | 4.890 | 1.064 | 0.902 | 2.047 |
| SBCI3 | 4.051 | 1.561 | 0.888 | 2.450 |
| SBCI4 | 4.902 | 1.168 | 0.904 | 1.021 |
| SBCI5 | 4.351 | 1.132 | 0.886 | 1.321 |
| SBCI6 | 4.968 | 1.268 | 0.944 | 1.255 |
| **Punishment Severity** | PS1 | 4.218 | 1.361 | 0.987 | 0.863 | 0.882 | 0.901 | 1.270 |
| **Detection Certainty** | DC1 | 4.410 | 1.404 | 0.929 | 0.782 | 0.802 | 0.822 | 1.413 |

[Note: AVE = Average Variance Extracted, SD = Standard Deviation, CR = Composite Reliability]

**Table 6**  The correlation matrix for Fornell-Larcker discriminant validity

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | AW | DC | DN | PS | PSSB | PV | RC | RE | SB | SBCL | SE | SN | SPA | SPCI |
| AW | **0.896** |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DC | 0.262 | **1.000** |  |  |  |  |  |  |  |  |  |  |  |  |
| DN | 0.464 | 0.259 | **0.857** |  |  |  |  |  |  |  |  |  |  |  |
| PS | 0.244 | 0.373 | 0.139 | **1.000** |  |  |  |  |  |  |  |  |  |  |
| PSSB | 0.476 | 0.575 | 0.454 | 0.468 | **0.803** |  |  |  |  |  |  |  |  |  |
| PV | 0.453 | 0.405 | 0.434 | 0.267 | 0.478 | **0.917** |  |  |  |  |  |  |  |  |
| RC | 0.276 | 0.176 | 0.267 | 0.059 | 0.208 | 0.316 | **0.946** |  |  |  |  |  |  |  |
| RE | 0.493 | 0.291 | 0.527 | 0.151 | 0.760 | 0.466 | 0.390 | **0.942** |  |  |  |  |  |  |
| SB | 0.396 | 0.188 | 0.645 | 0.284 | 0.393 | 0.410 | 0.238 | 0.489 | **0.736** |  |  |  |  |  |
| SBCL | 0.467 | 0.223 | 0.493 | 0.191 | 0.727 | 0.790 | 0.445 | 0.318 | 0.526 | **0.963** |  |  |  |  |
| SE | 0.677 | 0.381 | 0.661 | 0.266 | 0.604 | 0.625 | 0.315 | 0.611 | 0.592 | 0.461 | **0.915** |  |  |  |
| SN | 0.727 | 0.353 | 0.736 | 0.262 | 0.623 | 0.585 | 0.338 | 0.506 | 0.627 | 0.447 | 0.525 | **0.922** |  |  |
| SPA | 0.334 | 0.199 | 0.353 | 0.083 | 0.410 | 0.481 | 0.446 | 0.500 | 0.243 | 0.383 | 0.615 | 0.528 | **0.914** |  |
| SPCI | 0.275 | 0.109 | 0.224 | 0.043 | 0.250 | 0.334 | 0.682 | 0.341 | 0.135 | 0.324 | 0.482 | 0.432 | 0.801 | **0.901** |

**Table 7** The HTMT correlation matrix

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | AW | DC | DN | PS | PSSB | PV | RC | RE | SB | SBCL | SE | SN | SPA | SPCI |
| AW |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DC | 0.757 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| DN | 0.472 | 0.651 |  |  |  |  |  |  |  |  |  |  |  |  |
| PS | 0.240 | 0.373 | 0.800 |  |  |  |  |  |  |  |  |  |  |  |
| PSSB | 0.461 | 0.596 | 0.442 | 0.779 |  |  |  |  |  |  |  |  |  |  |
| PV | 0.444 | 0.404 | 0.430 | 0.263 | 0.570 |  |  |  |  |  |  |  |  |  |
| RC | 0.280 | 0.176 | 0.268 | 0.059 | 0.199 | 0.810 |  |  |  |  |  |  |  |  |
| RE | 0.495 | 0.290 | 0.532 | 0.151 | 0.458 | 0.468 | 0.591 |  |  |  |  |  |  |  |
| SB | 0.013 | 0.190 | 0.253 | 0.290 | 0.391 | 0.415 | 0.240 | 0.690 |  |  |  |  |  |  |
| SBCL | 0.467 | 0.223 | 0.493 | 0.191 | 0.322 | 0.787 | 0.446 | 0.220 | 0.641 |  |  |  |  |  |
| SE | 0.274 | 0.381 | 0.662 | 0.265 | 0.202 | 0.622 | 0.312 | 0.611 | 0.501 | 0.460 |  |  |  |  |
| SN | 0.231 | 0.355 | 0.739 | 0.265 | 0.421 | 0.586 | 0.338 | 0.509 | 0.299 | 0.451 | 0.718 |  |  |  |
| SPA | 0.332 | 0.198 | 0.355 | 0.083 | 0.410 | 0.481 | 0.445 | 0.502 | 0.239 | 0.382 | 0.612 | 0.526 |  |  |
| SPCI | 0.274 | 0.109 | 0.222 | 0.042 | 0.250 | 0.333 | 0.283 | 0.341 | 0.142 | 0.324 | 0.480 | 0.432 | 0.699 |  |

*5.3**. Testing the structural model and hypothesis*

The bootstrapping approach with 5000 resamples was used to test the structural model and hypotheses (Hair et al., 2014). Table 8 displays the significance values for the path coefficients, p-values, and t-statistics among the components.

**Table 8**  Structural model path analysis

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Hypothesis  and  Relationships | Path Coefficient  (β-value) | p-value | t-statistic | Results | R-square | Q-square | f-square |
| H1:  PV→SBCL | 0.659 | 0.000 | 7.027 | Supported | 0.428  0.720  0.116  0.180 | 0.411  0.575  0.100  0.004 | 0.063 |
| H2:  PSS→SBCL | 0.148 | 0.000 | 1.605 | Supported | 0.003 |
| H3:  RC→SPCI | 0.429 | 0.000 | 5.002 | Supported | 0.024 |
| H4:  SE→SPCI | 0.351 | 0.000 | 2.358 | Supported | 0.217 |
| H5:  RE→SPCI | 0.517 | 0.000 | 0.058 | Supported | 0.001 |
| H6:  SBCL→SPCI | 0.333 | 0.000 | 4.024 | Supported | 0.201 |
| H7:  SPA→SPCI | 0.667 | 0.000 | 7.741 | Supported | 0.031 |
| H8:  SN→SPCI | 0.177 | 0.000 | 0.240 | Supported | 0.010 |
| H9:  DN→SPCI | 0.102 | 0.000 | 0.012 | Supported | 0.023 |
| H10:  AW→SPA | 0.334 | 0.000 | 4.058 | Supported | 0.006 |
| H11:  PS→SPCI | 0.023 | 0.000 | 3.144 | Supported | 0.071 |
| H12:  DC→SPCI | -0.076 | 0.000 | 0.004 | Not Supported | 0.034 |
| H13:  SPCI→SB | 0.135 | 0.000 | 2.022 | Supported | 0.349 |

Perceivedvulnerability (β = 0.659, t = 7.027, p=0.000) and Perceived severity (β = 0.148, t = 1.605, p=0.000) were positively related to Security breach concern level and supporting Hypothesis H1 and H2. Hypothesis (H3) stated that, Response cost (β = 0.429, t = 5.002, p=0.000) was positively related to Security policy compliance intention and this hypothesis was also supported. Similarly, we assessed the variables of Security policy compliance intention and found that the hypothesis (H4) Self-efficacy (β = 0.351, t = 2.358, p=0.000), (H5) Response Efficacy (β = 0.517, t = 0.058, p=0.000), (H6) Security breach concern level (β = 0.333, t = 4.024, p=0.000), (H7) Security policy attitude (β = 0.667, t = 7.741, p=0.000), (H8) Subjective norm (β = 0.177, t = 0.240, p=0.000), (H9) Descriptive norm (β = 0.102, t = 0.012, p=0.000), (H10) Awareness (β = 0.334, t = 4.058, p=0.000), and (H11) Punishment severity (β = 0.023, t = 3.144, p=0.000), all had a positive impact on the intention respectively, and were statistically supported.

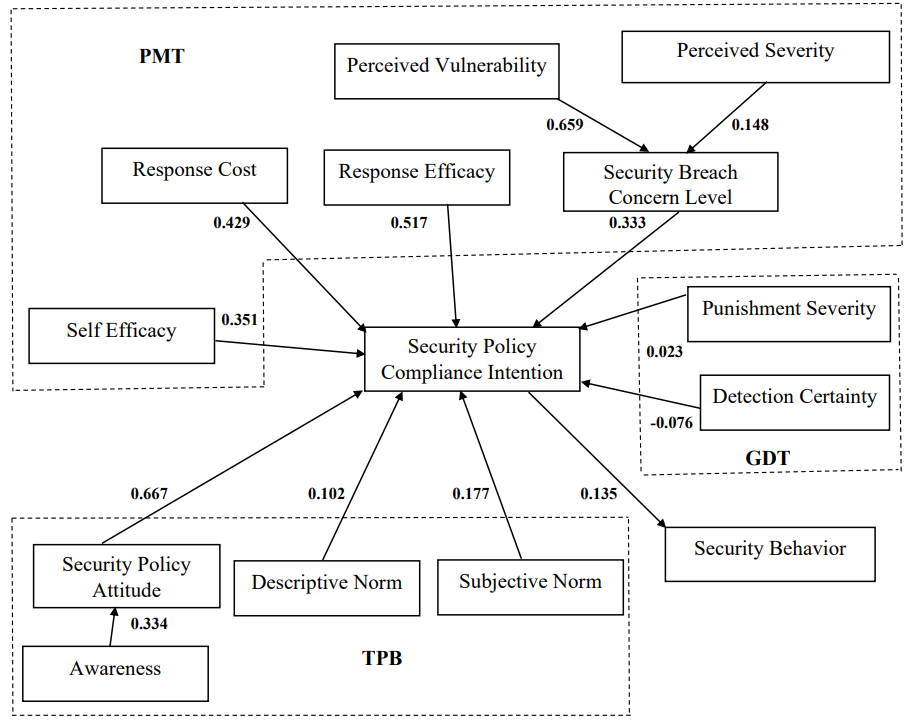
On the other hand, the predictors we examined of policy intention found that the hypothesis (H12) Detection Certainty (β = -0.076, t = 0.004, p=0.000) was not a positive impact on Security policy compliance intention and not statistically supported. Finally, hypothesis (H13) stated that, Security policy compliance intention (β = 0.135, t = 2.022, p=0.000) had positive effects on Security behavior and this hypothesis was statistically supported.

Additionally, we examined the effect of (f-square), cross-validated redundancy (Q-square), and the amount of variation explained (R-square). The values of (R-square) for Security Breach Concern Level, Security Behavior, Security Policy Attitude, and Security Policy Compliance Intention were 0.428, 0.180, 0.116, and 0.720, respectively. All the values of (R-square) were indicating the level of acceptance based on the cutoff (Cohen, 1977).

The cross-validated redundancy (Q-square) criterion is another key factor in assessing the accuracy of a model. The values of (Q-square) are determined by a blindfold technique in order to determine the prediction efficiency of exogenous constructs for endogenous constructs (Merli et al., 2019). It also evaluates the fitness of a model. Table 8 presents the (Q-square) value of predictive relevance, where the values of (Q-square) for Security Policy Compliance Intention, Security Breach Concern Level, Security Behavior, and Security Policy Attitude, and were 0.575, 0.411, 0.004, and 0.100 respectively. It was above zero (0), indicating that the predictive relevance of the model is satisfactory (Koohang et al., 2021; Ramayah et al., 2017).

For the purpose of evaluating the change in R-square by removing a particular extraneous variable from the model, the effect size (f-square) is measured, and the acceptance level is given as follows: (a) 0.15 medium effect; (b) 0.35 large effect; and (c) 0.02 small effect size (Cohen, 1977).

In this study, we found that Perceived Severity and Perceived Vulnerability were (f-square of 0.003) and (f-square of 0.063). It exerted a small effect on Security Breach Concern Level. Similarly, Response Cost, Subjective Norm, Response Efficacy, Security Policy Attitude, Punishment Severity, Descriptive Norm, and Detection Certainty were the value of (f-square = 0.024), (f-square = 0.010), (f-square = 0.001), (f-square = 0.031), (f-square = 0.071), (f-square = 0.023), and (f-square = 0.034) respectively and they all had a small effect on Security Policy Compliance Intention. On the other hand, Self-Efficacy, and Security Breach Concern Level were the value of (f-square = 0.217), and (f-square = 0.201), respectively and they had considered a medium effect on the intention. Security Policy Compliance Intention was (f-square of 0.349) a substantial large effect on Security Behavior. Finally, Awareness was (f-square of 0.006) and had a small effect on Security Policy Attitude. The model has small, medium, and high effect sizes, listed in Table 8. Figure 2 depicts the structural model that explains the path coefficients.



**Figure 2.** Structural Model

**6. Discussion**

Most countries with advanced technology employ PMT, TPB, and GDT when performing studies on user security behaviour in workplace and home settings. We employed a combined framework model that included the security behavior construct as well as the PMT, TPB, and GDT constructs to better understand the factors influencing students' security intention. The findings reveal that just one out of a total of thirteen hypotheses is not significant. The discussion section presents the findings of the research survey. Here, we will examine the relevance of each factor found in the data.

*6.1.* *Connection between protection motivation theory and security policy compliance intention*

Findings from this research showcase that PMT is one of the most effective theoretical frameworks for describing intentions to follow cyber security policies, which is consistent with other studies (Herath & Rao, 2009; Rogers, 1975). The results also represent that all hypotheses are significant for PMT, which indicates that this theory was appropriate for the data collected. Response Efficacy, Perceived Severity, Response Cost, Perceived Vulnerability, Security Breach Concern Level, and Self-Efficacy were all significant factors in determining the security policy compliance intention of PMT. In the PMT construct, self-efficacy was discovered to be a major predictor of students' behavioral intentions. The outcomes of other investigations are supported by that finding (Ifinedo, 2012; Mills & Sahi, 2019; Woon et al., 2005). Perceived vulnerability and perceived severity, two elements of the PMT threat appraisal, were correlated with students' security breach concern levels. This finding was satisfactory in that if a person assesses the threat, they plan to take precautionary measures for their own safety. Previous studies showed that there is a significant correlation between threat appraisal components and security intentions (Mills & Sahi, 2019; Sommestad et al., 2015; Woon et al., 2005). Also, security breach concern level has been shown to be significantly associated with compliance intentions.

In addition, response efficacy and response cost, two components of the coping appraisal of PMT, had a significant relationship with intention. A majority of past studies had established strong connections between response efficacy and intention (Mills & Sahi, 2019; Woon et al., 2005). The correlation between response efficacy and security intention were found to be important in specific behaviors relative to general behavior, according to a statistical analysis of PMT (Sommestad et al., 2015).

*6.2.* Theory of planned behavior and security policy compliance intention

The relationship of TPB constructs was also examined. In this research, TPB was tested for influence on student intentions to comply with security policies. According to the results of this study, attitudes had a substantial impact on university students intentions to comply with security measures. These findings are similar to those of earlier studies (Bulgurcu et al., 2010; Farooq, Ndiege, et al., 2019; Rivis & Sheeran, 2003). The results indicated that attitude is significantly impacted by security policy awareness. This outcome matches up with what has been seen in other research (Bulgurcu et al., 2010; Rocha Flores & Ekstedt, 2016; Thompson et al., 2017). Being aware of the risk and expense of information leaks can motivate individuals to adopt security practices. Subjective norms are deployed in TPB, and it was anticipated that they would affect the students security policy compliance intentions. However, we were able to identify significant relationship between subjective norms and security policy compliance intentions. The substantial correlation of subjective norms was also noted in previous research (Jansen & Van Schaik, 2017; Vance et al., 2012). Descriptive norms and security intentions showed a statistically significant association, similar to that of subjective norms. This outcome was similar to past findings where descriptive norms strongly influenced security policy compliance intentions (Jansen & Van Schaik, 2017; Vance et al., 2012).

*6.3. Theory of general deterrence and security intention*

In examining the deterrence factors effectiveness, it was discovered that punishment severity has a significant effect on intentions. Students are inclined to adhere to safety policies if they believe that there is a strong possibility of being arrested for breaking security rules. It was surprising to observe that detection certainty affected security policy compliance intentions negatively. In the literature on IS security, different consequences of punishment have been shown (Kankanhalli et al., 2003; Pahnila et al., 2007). Our analysis shows that detection certainty is less significant than the presence of punishment severity and its visibility.

*6.4. Security policy compliance intention and security behavior*

In our study, we discovered a significant correlation between behavioral intention and security behavior. Compliance with IS security policies is largely dependent on human behavior. Other studies also found a link between security intention and security behavior (Ali et al., 2021; Dinev et al., 2009; Pahnila et al., 2007). Behavioral determinants including a strong security culture, good security knowledge, efficient security management, and other security behaviors improve student compliance with the cyber security policy. In addition to enhancing security behavior, analyzing the reasons for and potential remedies for students' compliance intents is crucial.

Finally, the findings imply that the PMT and TPB frameworks are the best predictors of intentions to abide by cyber security policies. This is due to the importance of all of the main predictors from both the PMT and TPB, which included perceived vulnerability, self-efficacy, perceived severity, response cost, security breach concern level, and response efficacy. This idea holds that students will be more likely to adhere to cyber security policies if they are particularly exposed to and threatened by information security threats and are knowledgeable about the proper course of action. The results of the study, in general, are consistent with this justification. The study's findings showed a weak relationship between GDT and intention. The reason for this is that only penalty severity, one of the two GDT components, significantly predicted whether or not students would adopt security policies.

**7. Conclusion**

This study's objective was to assess the variables that affect undergraduate students' security behavior. An integrated model that includes components of the TPB, PMT, and GDT was created on the basis of the literature evaluation in this context. Empirical findings from a PLS-SEM analysis with 519 individuals showed that our integrated model validated 12 of the 13 assumptions. The results show that among college students, intention was shown to be the most powerful predictor of security behavior with the biggest effect size. This suggests that if students feel they have no control over their personal information and believe it is constantly a target of attack, they are highly driven to adhere to cyber security standards. Our research also showed that PMT and TPB are the most useful frameworks for undergraduate students to comprehend compliance with cyber security policy. Only harshness from the other GDT elements had a stronger correlation with the intention to follow security policy. On the other hand, the intention to comply with security policy was not significantly impacted by the detection certainty from GDT. Finally, it was established that behavioral intention and security behavior had a strong correlation.

**References**

Abramovaite, J., Bandyopadhyay, S., Bhattacharya, S., & Cowen, N. (2022). Classical deterrence theory revisited: An empirical analysis of Police Force Areas in England and Wales. European Journal of Criminology. https://doi.org/10.1177/14773708211072415

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. *Action Control*, 11–39. https://doi.org/10.1007/978-3-642-69746-3\_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akers, R. L. (1973). Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. In *Source: The Journal of Criminal Law and Criminology* (Vol. 81, Issue 3). Autumn. http://www.jstor.orgURL:http://www.jstor.org/stable/1143850

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 8). MDPI AG. https://doi.org/10.3390/app11083383

Al-Omari, A., El-Gayar, O., Deokar, A., & AL-Omari, A. (2012). Information Security Policy Compliance: The Role of Information Security Awareness. *Proceedings of the 18th Americas Conference on Information Systems (AMCIS)*, *1*. http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16

Alyoussef, I. Y. (2022). Acceptance of a flipped classroom to improve university students’ learning: An empirical study on the TAM model and the unified theory of acceptance and use of technology (UTAUT). *Heliyon*, *8*(12). https://doi.org/10.1016/j.heliyon.2022.e12529

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer. In *Source: MIS Quarterly* (Vol. 34, Issue 3).

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. In *Source: MIS Quarterly* (Vol. 22, Issue 1).

Beck, L., & Ajzen, I. (1991). Predicting Dishonest Actions Using the Theory of Planned Behavior. In *JOURNAL OF RESEARCH IN PERSONALITY* (Vol. 25).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 523–548. https://doi.org/10.2307/25750690

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*. https://doi.org/10.1109/HICSS.2009.74

Chiesi, F., Bonacchi, A., Lau, C., Tosti, A. E., Marra, F., & Saklofske, D. H. (2020). Measuring self-control across gender, age, language, and clinical status: A validation study of the Italian version of the Brief Self-Control Scale (BSCS). *PLoS ONE*, *15*(8 August 2020). https://doi.org/10.1371/journal.pone.0237729

Chingos, M. M., Griffiths, R. J., Mulhern, C., & Spies, R. R. (2017). Interactive Online Learning on Campus: Comparing Students’ Outcomes in Hybrid and Traditional Courses in the University System of Maryland. *Journal of Higher Education*, *88*(2), 210–233. https://doi.org/10.1080/00221546.2016.1244409

Chin, W. W. (1998). *The Partial Least Squares Approach to Structural Equation Modeling.* Modern Methods for Business Research. https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1527177

Cohen, J. (1977). Statistical power for the behaviour sciences. In *Hillsdale, NJ: Laurence Erlbaum and Associates*. http://www.sciencedirect.com:5070/book/9780121790608/statistical-power-analysis-for-the-behavioral-sciences

Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Information Systems Management*, *36*(4), 306–322. https://doi.org/10.1080/10580530.2019.1651113

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 23. https://doi.org/10.17705/1jais.00133

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, 5257–5261. https://doi.org/10.1145/2858036.2858265

Ernovianti, E., Kamariah Nik Mat, N., Kassim, U., Rashid, R., & Syaheera Meor Shaari, M. (2012). The Usage of Internet Banking Service Among Higher Learning Students in Malaysia. *American Journal of Economics*, *2*(4), 105–108. https://doi.org/10.5923/j.economics.20120001.24

Farooq, A., Jeske, D., & Isoaho, J. (2019). Predicting Students’ Security Behavior Using Information-Motivation-Behavioral Skills Model. *IFIP Advances in Information and Communication Technology*, *562*, 238–252. https://doi.org/10.1007/978-3-030-22312-0\_17

Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019). Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. *IEEE AFRICON Conference*, *2019-September*. https://doi.org/10.1109/AFRICON46755.2019.9133764

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, *17*(4), 199–209. https://doi.org/10.1016/j.istr.2013.03.004

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. In *Source: Journal of Marketing Research* (Vol. 18, Issue 1).

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. In *European Business Review* (Vol. 31, Issue 1, pp. 2–24). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. In *European Business Review* (Vol. 26, Issue 2, pp. 106–121). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-10-2013-0128

Hanus, B., & Wu, Y. “Andy.” (2016). Impact of Users’ Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/J.1540-5915.2012.00361.X

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ICS-03-2017-0018

Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. *New Media and Society*, *18*(9), 2063–2079. https://doi.org/10.1177/1461444815577797

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Ketchen, D. J. (2013). A Primer on Partial Least Squares Structural Equation Modeling. *Long Range Planning*, *46*(1–2), 184–185. https://doi.org/10.1016/j.lrp.2013.01.002

Kirsch, L., & Boss, S. (2007). The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines. *International Conference on Information Systems, ICIS*. http://aisel.aisnet.org/icis2007

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. In *International Journal of e-Collaboration* (Vol. 11, Issue 4).

Koohang, A., Nord, J. H., Sandoval, Z. V., & Paliszkiewicz, J. (2021). Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. *Journal of Computer Information Systems*, *61*(2), 99–107. https://doi.org/10.1080/08874417.2020.1779151

Lankton, N. K., Stivason, C., & Gurung, A. (2019). Information protection behaviors: morality and organizational criticality. *Information and Computer Security*, *27*(3), 468–488. https://doi.org/10.1108/ICS-07-2018-0092

Lee, N., Kim, J., Kim, E., & Kwon, O. (2017). The Influence of Politeness Behavior on User Compliance with Social Robots in a Healthcare Service Setting. *International Journal of Social Robotics*, *9*(5), 727–743. https://doi.org/10.1007/s12369-017-0420-0

Loch, K. D., Conger, S., & Oz, E. (1998). Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics. In *Source: Journal of Business Ethics* (Vol. 17, Issue 6).

Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2022). Blockchain adoption: A study of cognitive factors underpinning decision making. *Computers in Human Behavior*, *131*. https://doi.org/10.1016/j.chb.2022.107207

Melović, B., Stojanović, A. J., Backović, T., Dudić, B., & Kovačičová, Z. (2020). Research of attitudes toward online violence— significance of online media and social marketing in the function of violence prevention and behavior evaluation. *Sustainability (Switzerland)*, *12*(24), 1–24. https://doi.org/10.3390/su122410609

Merli, R., Preziosi, M., Acampora, A., & Ali, F. (2019). Why should hotels go green? Insights from guests experience in green hotels. *International Journal of Hospitality Management*, *81*, 169–179. https://doi.org/10.1016/j.ijhm.2019.04.022

Mills, A. M., & Sahi, N. (2019). An Empirical Study of Home User Intentions towards Computer Security. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-January*, 4834–4840. https://doi.org/10.24251/HICSS.2019.583

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees’ behavior towards IS security policy compliance. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2007.206

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, *20*(1), 153–177. https://doi.org/10.1080/07421222.2003.11045759

Purwanto, A., & Sudargini, Y. (2021). Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review. *Journal of Industrial Engineering & Management Research*, *2*(4). https://doi.org/10.7777/jiemar.v2i4

Qing, H. U., & Dinev, T. (2005). Is spyware an internet nuisance or public menance? In *Communications of the ACM* (Vol. 48, Issue 8, pp. 61–66). https://doi.org/10.1145/1076211.1076241

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Menon, M. A. (2017). Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0. *Pearson Malaysia Sdn Bhd*, *July*, 587–632. https://www.researchgate.net/publication/312460772\_Partial\_Least\_Squares\_Structural\_Equation\_Modeling\_PLS-SEM\_using\_SmartPLS\_30\_An\_Updated\_and\_Practical\_Guide\_to\_Statistical\_Analysis

Rasoolimanesh, S. M. (2022). Discriminant validity assessment in PLS-SEM: A comprehensive composite-based approach. *Data Analysis Perspectives Journal*, *3*(2), 1–8. https://www.scriptwarp.com,

Reddy, D., & Rao, V. (2016). Cybersecurity Skills: The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance. *AMCIS 2016 Proceedings*. https://aisel.aisnet.org/amcis2016/ISSec/Presentations/23

Rivis, A., & Sheeran, P. (2003). Social influences and the theory of planned behaviour: Evidence for a direct relationship between prototypes and young people’s exercise behaviour. *Psychology and Health*, *18*(5), 567–583. https://doi.org/10.1080/0887044032000069883

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Safa, N. S., Ghani, N. A., & Ismail, M. A. (2014). An Artificial Neural Network Classification Approach For Improving Accuracy Of Customer Identification In E-Commerce. In *Malaysian Journal of Computer Science* (Vol. 27, Issue 3).

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Saputra, N., Sari, R., Langsa, I., Sahir, S., Patimah, S., Intan, Uinr., Safriadi, radenintanacid, & Ar-Raniry, U. (2021). Learning Agility and Digital Quotient View project Competence of PMO Leader View project PRO-SOCIAL BEHAVIOR ON SME RESILIENCE: SME’S LEADERSHIP IN OVERCOMING COVID-19 CRISIS. *Ilkogretim Online-Elementary Education Online, Year*, *20*(4), 832–838. https://doi.org/10.17051/ilkonline.2021.04.90

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Sari, P. K., Nurshabrina, N., & Candiwan. (2016). Factor analysis on information security management in higher education institutions. *Proceedings of 2016 4th International Conference on Cyber and IT Service Management, CITSM 2016*. https://doi.org/10.1109/CITSM.2016.7577518

Sheeran, P., & Orbell, S. (1999). Augmenting the Theory of Planned Behavior: Roles for Anticipated Regret and Descriptive Norms1. In *Journal of Applied Social Psychology* (Vol. 29).

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Sobaih, A. E. E., & Elshaer, I. A. (2022). Personal Traits and Digital Entrepreneurship: A Mediation Model Using SmartPLS Data Analysis. *Mathematics*, *10*(21). https://doi.org/10.3390/math10213926

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-Analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. https://doi.org/10.4018/IJISP.2015010102

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19–34. https://doi.org/10.1016/J.COSE.2014.02.010

Tangney, J. P., Boone, A. L., & Baumeister, R. F. (2018). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. In *Self-Regulation and Self-Control* (pp. 173–212). Routledge. https://doi.org/10.4324/9781315175775-5

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage. *Information Systems Research*, *6*(2), 144–176. https://doi.org/10.1287/ISRE.6.2.144

Thompson, N., & Mcgill, T. (2017). Mining the Mind – Applying Quantitative Techniques to Understand Mental Models of Security. *ACIS 2017 Proceedings*. https://aisel.aisnet.org/acis2017/50

Thompson, N., McGill, T. J., & Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. *Computers and Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, V., Brown, S. A., & Smith, R. H. (2001). A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges Venkatesh and Brown/Personal Computers in Homes MIS OLarter1y A LONGITUDINAL INVESTIGATION OF PERSONAL COMPUTERS IN HOMES: ADOPTION DETERMINANTS AND EMERGING CHALLENGES1. In *Source: MIS Quarterly* (Vol. 25, Issue 1).

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Wash, R., & Rader, E. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Symposium On Usable Privacy and Security (SOUPC)*, 309–325.

Williams, K. R., & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. In *Source: Law & Society Review* (Vol. 20, Issue 4).

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–341. https://doi.org/10.1080/108107396127988

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings*. https://aisel.aisnet.org/icis2005/31

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yakubova, G., Hughes, E. M., & Hornberger, E. (2015). Video-Based Intervention in Teaching Fraction Problem-Solving to Students with Autism Spectrum Disorder. *Journal of Autism and Developmental Disorders*, *45*(9), 2865–2875. <https://doi.org/10.1007/s10803-015-2449-y>

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science, 43*, 115-135.

Ab Hamid, M. R., Sami, W., & Sidek, M. M. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *In Journal of Physics: Conference Series* (Vol. 890, No. 1, p. 012163). IOP Publishing.