Management Research Spectrum
ISSN: 2659-1960 (Online)
ISSN: 2659-1871 (Print)

An Information Security Framework for Higher Education Institutions based on Theories of Protection Motivation and Planned Behaviour

Bala Salisu[1]*

[1] *School of Management Studies, The Federal Polytechnic Damaturu, 620001 Damaturu, Yobe State, Nigeria*

* Corresponding author: bs.bala.ng@gmail.com

Abstract

This study presents a conceptual framework for examining behavioural intention as a mediator (and employee concern for securing information assets as moderator) between employees' dispositional factors (perceived security self-efficacy, perceived security response self-efficacy, security attitude, subjective security norms) and their willingness to take protective actions in securing the information assets of Nigerian higher educational institutions (HEIs) from threats to ensure confidentiality, integrity and continuity in the system. The general aim of the study is to produce an information systems security framework for protecting the confidentiality, integrity, and accessi-bility of information assets in Nigerian HEIs, thereby averting unauthorised access, use, disclosure, destruction, alteration or damage of information assets. The significance of the study lies in providing researchers and policy makers with a framework for addressing information security matters in HEIs.

Keywords: *Information Security, H, Protection Motivation Theory, Theory of Planned Behaviour, Nigeria.*

Article Information:

Received: 5 December 2021
Revised: 10 February 2022
Accepted: 15 February 2022
Published: 2022

Vol. 12, No. 1, 2022

Introduction

In the rapidly evolving higher education sector, where institutions increasingly rely on digital technologies and data-driven processes, information security has emerged as a paramount concern (Ovelgönne *et al.*, 2017). The safeguarding of sensitive information, such as student records, research data, and administrative documents, has become an imperative for the continued functioning and reputation of these institutions. With the ever-growing threat of cyberattacks and data breaches, it is imperative for higher education institutions (HEIs) to develop robust information security frameworks that not only protect their digital assets but also promote a culture of security among their stakeholders (Mello, 2018).

Information security is a composite of four key elements: namely, people, processes, policies, and technologies (Hagen *et al.*, 2008). It relies on the synergy of these elements, where people's awareness and proactive actions, well-designed processes, pragmatic policies, and cutting-edge technologies work together harmoniously to safeguard an institution's information assets and maintain their confidentiality, integrity, and availability (Winjum and Mølmann, 2008). This integrated approach not only provides a robust defence against a wide range of cyber threats but also fosters a culture of security within an organization, ensuring that information remains secure in the face of constantly evolving challenges. Thus, considering the complex structure of information security systems and its diverse concepts, it becomes obvious that developing a single framework capturing all the significant domains may not be worthwhile. Accordingly, researchers are always advised to proceed with caution by taking sets of manageable variables at a time that closely explain aspects of the systems. In this study, the researcher follows the observation of Sasse *et al.* (2001) that the human factor is the weakest link in information security and therefore focus on the behavioural (human) aspect of information security.

This conceptual paper presents an innovative approach to address the challenges of information security in HEIs by integrating two prominent psychological theories: Protection Motivation Theory (PMT) (Rogers, 1975) and Theory of Planned Behaviour (TPB) (Ajzen, 2015). PMT helps us understand the cognitive processes that underlie individuals' decisions to engage in protective behaviours, while TPB sheds light on the factors influencing intention and behaviour. the combined explanatory power of these two theories was used to guide development of the information security framework tailored to the unique context of Nigerian HEIs. The significance of this research lies in its potential to provide HEIs with a structured and psychologically informed approach to enhance information security. This framework not only focuses on technological aspects but also emphasises the role of human behaviour and motivation in safeguarding sensitive institutional data.

Information Systems Security in Nigerian HEIs

Information is the lifeblood of higher education intuitions. They created data, use data, and keep data. Some of these data are commonplace but a vast majority of the data are proprietary and personal and include information on research projects, employee records, students' academic records and sensitive correspondences. Universities sit on rich data assets, including students' personal and academic records, economically viable research data, personal data of university employees, financial data of the university, and university correspondences. In particular, the research data in universities are immensely valuable and can make huge impact by giving those who access them profitability, competitive advantage and also can support national interest in education, industry, health and defence (Pascual, 2009). Indeed, universities are centres of excellence awash in creative thought and innovation – all stored as information in various media and repositories. Thus, universities have information assets that are huge and valuable.

In view of the foregoing, little wonder that the state of information systems security in Nigerian HEIs is low indeed. In general, information systems security risks can emerge from can come from inside or outside (Walton and Limited, 2006) the universities. Insider threats may emerge as theft of information by employees for financial gain, hedonism, revenge against colleagues or the system, or it can be inadvertent. Outsider threats to CI may be motivated by corporate espionage, competitive intelligence gathering by adversaries, or sponsored by activist groups, media houses, or rival political interests. In fact, the outsiders are legion, and they already have the motive to attack and the means to do so; they are only waiting for the opportune time.

Data Sources Utilised

In developing the conceptual, materials were sourced from several academic databases including Association for Information Systems database (https://aisnet.org/), Clarivate's Web of Science, Elsevier's Scopus, and Google Scholar. Additionally, the databases of leading academic publishers were also explored, including Taylor and Francis Online, ScienceDirect, Emerald Insight, SAGE Online, Springer, and Inderscience. In addition to these sources, further materials were sourced from the website of the National Information Technology Development Agency (NITDA) (https://nitda.gov.ng/), especially the *Nigeria Data Protection Regulation 2019* (NITDA, 2019b) and the *Framework and Guidelines for Information and Communication Technology (ICT) Adoption in Tertiary Institutions* (NITDA, 2019a). These documents were collectively utilised to in developing the conceptual framework for information systems security in Nigerian HEIs.

Theoretical Background

The researcher started this review chapter with identifying the relevant theories that could explain the human dynamics influencing the protection of institutional information assets from threats. A theory is "a set of interrelated constructs (concepts), definitions, and propositions that present a systematic view of phenomena by specifying relations among variables, with the purpose of explaining and predicting the phenomena" (Kerlinger and Lee, 2000, p. 11). Many theories have been developed and or used to explain issues in the field of information security. Larsen and Eargle (2015) compiled summaries of 138 theories used in information security research on the website of the popular Association of Information Systems (AIS). However Ajzen's (2015) Theory of Planned Behaviour (TPB) and Rogers' (1975) Protection Motivation Theory (PMT) stand as the most esteemed and dependable frameworks, encompassing elements such as subjective norms, self-efficacy, attitudes, perceived benefits, threat vulnerability, threat severity, response efficacy, response cost, and practical experience.

In view of the foregoing, this study proposes to employ the PMT and the TBP as the study's underpinning grids. This is because researchers generally employ the PMT in addressing "any situation involving threat" (Rogers, 1983, p. 172), while the TPB is widely used in explaining human attitudes and behaviours Rogers (1983). Thus, the PMT and TPB were collectively used in this study to provide a theoretical lens for developing a framework for explaining the protective behaviours of employees in the context of threats challenging information systems security managers in HEIs.

Protection Motivation Theory (PMT)

Propounded in the context of healthcare by Rogers (1975) explaining the influence of threat and coping appraisal on protection intention [and later extended in Rogers (1983) to study behaviour], the PMT is now a well-established framework for investigating information-related security matters. The PMT mainly explains threat assessment and coping assessment. Threat assessment is a combination of two factors: perceived vulnerability to the likelihood of threatening events occurring and the severity of the event's consequences. Threat coping assessments have a three-factor structure. These are (1) self-efficacy (which is the employee's ability to cope with or perform the proposed behaviour), (2) response effectiveness (which is the employee's belief about the perceived usefulness of their action), and (3) cost estimates (which time, effort, money, training and others) and response cost (which is perceptions about the benefits of the perceived opportunity) (Kothe *et al.*, 2019). The core constructs of the PMT is illustrated in Figure 1.

Source: Rogers (1983, p. 168)
Figure 1. Core Constructs of the PMT

The PMT considers the need to engage in one of two types of behaviour in response to a threat, either adaptive or inappropriate. Adapted behaviour is a type of behaviour that is effective in protecting a person from a threat (coping appraisal), while inappropriate behaviour is doing nothing or engaging in behaviour that may increase risk (threat appraisal). In the threat assessment, individuals evaluate the probability of occurrence of the threat and the severity of the threat. The theory also assesses whether the behaviour can be an effective threat deterrent (Hanus and Wu, 2015).

Theory of Planned Behaviour (TPB)

As the expanded version of theory of reasoned action (TRA) (Ajzen and Fishbein, 2004), the focus of TPB is "intention," which provides an orientation to a behaviour. Intention shows how much an individual is willing and how much effort he plans to expend in order to exhibit a behaviour. The strength of the intention for a behaviour is in a sense an indicator of the performance to be exhibited. TPB posits that three variables affect intention: attitudes towards behaviour, subjective norms, and perceived behavioural control (Ajzen, 2015). Intention, in turn, determines behaviour. This sequence of influences is illustrated in Figure 2. Thus, there are altogether five constructs in the TPB: namely, attitudes, subjective norms, perceived behavioural control (predictor variables); intention (mediator); and behaviours (outcome variable).

The TPB is based on the idea that people make rational decisions by systematically accessing information. It assumes that the main determining factor of people's behaviour is the logical outcome of the cognitive process, and that three main elements through intention create individual behaviours. According to the TPB, employees' beliefs about the likely results of their behaviour and the significance of the results shape their attitude (Ajzen, 2015).

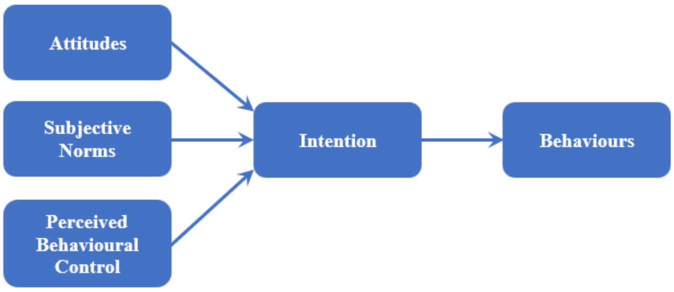


Figure 2. Theory of Planned Behaviour

Theoretical Integration

Addressing information systems security issues from the perspective of its weakest link (i.e., people) is overwhelmingly a motivational rather than technological challenge. Thus, the main theory driving this research is the PMT. However, explanatory power of the PMT can be assumed only when the same individual employee bears the cost of an action and the consequences of that action. It is settled science that nothing could be gained when nothing is ventured. Thus, employees can only engage in protective behaviours geared towards supporting information security measures when they expend the necessary time, energy and efforts (cost). In other words, the individual bears the cost of information security-compliant behaviours while the institution gets the benefits (consequences). Conversely, when an employee engages in anti-information security behaviours leading to information security violations and breaches, the cost is borne by the institution. Thus, a cost–consequence misalignment arises. This outcome is expected to generate tension, one of Kothe et al.'s (2019) three mechanisms of deviant affordance. This misalignment-induced tension between the costs and the consequences of information security behaviours weakens the explanatory power of the PMT. This study proposes to address this gap.

To bridge this cost–consequence gap, the TPB is integrated into the PMT, and the resulting model expanded with a coupling construct suggested from the extant literature. Several studies (e.g., Ifinedo, 2012; Wang *et al.*, 2019) have integrated the PMT with TPB to address their research questions. In general, integrating the TPB with PMT is justified on the established grounds that the TPB domain evinces the need improvements of sufficient magnitude to warrant adjusting it when used in information security research (Sommestad et al., 2015). However, Thus, this study draws on several empirical models to justify the use of behavioural intention (based on the assumptions of the TPB) and employee's level of concern for securing information assets (based on the PMT) as mediating and moderating variables, respectively, in bridging the costs–consequences gap identified in the PMT (see Table 1 for a summary of the models).

The first empirical model is Warkentin et al.'s (2016) Protective Security Behaviour Continuance Model which assert that an employee may engage in protective behaviour where they exhibit explicit intention to engage in information security-compliant behaviours. Employees' level of concern about information security, defined as the level of employee's engagement and appraisal of threatening information security matter, remains one of their five unstudied issued in the field of information security research. Also, D'Arcy and Greene (2014) theorised that culture and employee relationships contribute to information systems security, and this is possible where employees exhibit concern about the system. Finally, Yoon and Kim's (2013) Individual Security Behaviour Model supports the moral undertone (an employee's concern with the security of their institutional information system) that give fillip to self-efficacy (a TPB/PMT construct) critical in generating the desire information security behaviours from employees.

Table 1. Information Security Models with Focus on Employee Intentions

Author(s)	Models	Remarks
Warkentin et al. (2016)	Protective Security Behaviour Continuance Model	Warkentin et al. (2016) posit that threat severity, self-efficacy, threat susceptibility, and response efficacy are critical antecedents to information system security but must be supported by strong intention to exhibit motivated behaviour in favour of data security.
D'Arcy and Greene (2014)	Security Compliance Intention Model	D'Arcy and Greene (2014) explain that the combined effects of security culture and employee relationships contribute to information systems security.
Yoon and Kim (2013)	Individual Security Behaviour Model	Yoon and Kim (2013) view consider IT security from the employee's point of view and hold that the desire to promote information security rather than threat rests on their moral obligation and practice efficacy.

In synthesising the exogenous constructs of the two theories underpinning this study, the researcher relied on Ajzen's (1991) observation that perceived behavioural control (a construct of the TPB) and self-efficacy (a construct of the PMT) may not be discriminant valid, thereby suggesting that the two constructs are essentially the same. Thus, this study retains the most commonly used term self-efficacy in its information system security model. Similarly, so many researchers (Ifinedo, 2012; Lee, 2011) have employed the mediating construct intention (from the TPB) and its counterpart protection motivation (in the PMT) in operationalising the same referent, thereby suggesting close similarity between the two constructs. Thus, the study used the term protective intention to synthesise the two constructs.

In addition to synthesis of similar constructs between the PMT and the TPB, this research also looked into the intention–behaviour gap from the perspective of information security in HEIs. It

It is also interesting to note that in the health research field [within which Rogers (1975) first developed the PMT], fear is usually treated as a mediating factor between perceived vulnerability, perceived severity, and threat appraisal. However, critic's observations that fear messages do not work in other contexts such as workplaces, and that the reverse is often the case. Additionally, Imamov (2018) observe that information security threats are digital and employees' response to them tend to be a passive process that has to be motivated by a strong desire (or concern) to protect information assets or to mitigate the negative consequences of protection failure. Thus, there it seems that studies have missed out to include a catalysing mechanism that activates intention and imbue it with the power to generate desired behaviours. To this end, studies (e.g., Al Shikhy *et al.*, 2019) have suggested that conscientious employees are more susceptible to produce the relevant referent behaviour than employees not so conscientious. It is in line with this thinking that this study proposes to use employees' level of concern for securing information assets as a positive moderating influence in the protective intention–protective behaviour relationship, while at the same time functioning as a predictor variable to protective intension. It is line with such emerging results that recommend five new constructs missing from extant research, which include employees' concern for securing information assets. It is noteworthy that some other scholars have mooted this variable (i.e., employees' show of concern for securing information assets) but used it as exogenous construct rather that moderating variable. In this study, the researcher takes the position that employee's level of concern for securing information assets s could serve as a moderating mechanism in the PMT relationships (between predictor variables and the mediating variable), thereby strengthening (where it is high) or weakening (where it is low) the prospects of employees nursing protective intention and ultimately engaging in protective behaviours.

From the foregoing discourse, it seems that a moderated mediation model is most appropriate as an explanatory framework for information systems security in HEI. Accordingly, this study propose such a model using perceived security self-efficacy, perceived security response self-efficacy, security attitude, subjective security norms, protective intention, protective actions, employee concern for securing information assets, and protective actions. The interplay among these eight variables will be investigated according to their respective behaviours based on the typology suggested by the PMT and TPB. Thus, this study seeks to bridge this important gap by integrating the relevant constructs of the TPB into the PMT to develop a model for information systems security in Nigerian HEIs.

Conceptual Clarifications

In science, constructs should be defined in such a way that the indicators operationalising/defining them should be clear and unambiguous. According to Zwanenburg and Qureshi (2019), a well-defined construct has known indicators which could easily be measured. Constructs should therefore be properly defined for any study to merit the title of scientific inquiry. Conceptual definition is an essential requirement in identifying the appropriate procedures for validating construct measures and evaluating the measurement outcomes (Schwab, 2005).

Information Systems Security

Information systems security entails a series of measures and actions aimed at safeguarding both the information system itself and the data it contains (Niemimaa and Niemimaa, 2017).Thus, protection is the kernel of information security and its overriding objective. This protection is designed against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Elements of Information Systems Security (CIA)

The triad of information security objectives (confidentiality, integrity, availability) have been standardised by the US National Institute of Standards and Technology (NIST) in its Standards for Security Categorization of Federal Information and Information Systems (NIST, 2004). According to NIST (2004), confidentiality refers to "Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." A loss of confidentiality is the unauthorised disclosure of information. Confidentiality is lost when CI is disclosed in an unauthorised manner. The issue of confidentiality is tricky to deal with regards to the operations of a university. A university is an innovation and creativity centre populated by thinkers and purveyors of knowledge "who are open and free with thought and ideas" (Wood, 2014, p. 194). However, this very culture of openness exposes university to attacks by insiders and outsiders alike. (Liang *et al.*, 2016; Meng *et al.*, 2018). Generally, universities strive to adhere to the principles of open science , yet they must protect their sensitive and proprietary data from malicious people as well as personal data and data which has not yet been made public. The challenge here is to find a system of classifying information (and thus protecting sensitive university information) that does not at the same time stifles innovation and creativity by creating a silo mentality among key university stakeholders.

Table 2. Typology of Framework Variables

Predictor Variables	Mediating Variable	Moderating Variable	Criterion Variable
▪ Security Threat Susceptibility ▪ Security Threat Severity ▪ Perceived Security Response Efficacy ▪ Perceived Security Response Cost ▪ Perceived Security Efficacy ▪ Perceived Security Attitude ▪ Subjective Security Norms ▪ Concern for Securing Information Assets	Protective Security Intention	Concern for Securing Information Assets	Protective Security Actions

Integrity as the second of the three legs of securing CI in organisations. According to NIST (2004), integrity entails "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity." A loss of integrity is the unauthorised modification or destruction of information. Effort should be made to ensure that accident or malice cannot alter CI. The risks related to the integrity of the information come from the unauthorised disclosure (voluntary or accidental) and alteration via an intrusion into the IS of the organisation. Integrity relates directly to the interaction of the code, the object and meaning. Alteration of one of these three elements is enough to distort the information and destroy its integrity.

Several issues warrant universities to invest in upholding the integrity of their information assets. For example, Wood (2014) observes in the context of higher education that the risks to information integrity can emanate from university staff who may self-initiate data breach or may be compromised by external forces to steel data in return for some personal benefits. In another dimension, Universities partner with diverse external parties on various research projects whose details must not only be kept confidential but the results of the research must also be unquestionable in terms of integrity. The sustainability of such research collaborations depends on the authenticity of the method and the experimental data involved which must also be preserved and protected. Again, as public institutions, universities also have their financial books audited regulatory bodies. Indeed, Georg (2007) reports that "Integrity was judged to be most important from a regulatory point of view" (p. 224), thus supporting the importance of rules and regulatory factors as important antecedents of information security. It is apparent that the audit requirement cannot be achieved without ensuring the integrity of CI in universities. Modifications and inconsistencies in CI and other data indicates lack of integrity which my lead to adverse auditor judgement and concomitant bad reputation. Universities must therefore uphold the integrity of their information assets through a robust CI management system.

Finally, availability of CI is the last of the CIA triad and refers to “Ensuring timely and reliable access to and use of information” (NIST, 2004). A loss of availability is the disruption of access to or use of information or an information system. A common problem of availability with regards CI is denial of service, especially on digital platforms. Availability of CI is critical to the daily survival of organisations so that authorised persons are able to access and use the CI at all times in the service of clients. CI should be readily available to authorised personnel. Highly CI that is not made available to the authorised users as risky as CI that has been leaked. The availability principle is meant ensured that the information infrastructure in the organisation is maintained continuously to avoid unnecessary denial of service.

Models of Information Security for Ensuring CIA

IS models are designed for implementing the three principles of IS security (i.e., the CIA). This is why they are alternatively called the CIA maintenance models. There are three classical IS security models: namely, the Bell-LaPadula Model (addressing the issue of confidentiality), the Biba Model (concerned with integrity), and the Clarke-Wilson Security Model (dealing with accessibility). In other words, all policies, programs, including laws, should demonstrate the authenticity of electronic documents (preserving all characteristics of the original document), their reliability (ensuring the necessary document features and processing methods) to legally, administratively, and evidentially establish document identity. These policies and programs must also fully align with guidelines and standards, ensure the integrity of the document (including content, context, structure, and presentation), and ensure its usability with all types of information systems, including current and future e-government applications. These four fundamental attributes should be inherent in any such policies, programs, or legal frameworks (Duranti, 2002). It is also considered whether electronic documents with these features are managed in an effective and reliable system in order to fill their life cycle and meet the expectations of the institution. This system is called electronic document management system (ERMS).

Development of Hypotheses

Security Threat Susceptibility and Protective Security Intention

The study hypothesizes that there is a significant relationship between security threat susceptibility and protective security intention in the context of information security in HEIs. Specifically, the study posits that individuals who perceive themselves to be more susceptible to security threats, such as data breaches or cyberattacks, are more likely to exhibit a heightened intention to engage in protective security measures. This hypothesis is rooted in the PMT (Rogers, 1983), which suggests that individuals’ motivation to adopt protective behaviours is influenced by their perceived threat susceptibility. In the context of information security, it is anticipated that higher perceived susceptibility to security threats will lead to a stronger intention to proactively safeguard sensitive information through security measures and practices.

Security Threat Severity and Protective Security Intention

This hypothesis posits that there exists a significant correlation between perceived security response efficiency and individuals’ protective security intention within the realm of information security, particularly in the context of HEIs. Specifically, it suggests that individuals who perceive security response measures to be efficient and effective in addressing potential security threats are more likely to exhibit a heightened intention to engage in protective security behaviours. This hypothesis aligns with the PMT (Rogers, 1983), which suggests that the perceived effectiveness of protective responses influences one's motivation to adopt such responses. In information security, it is anticipated that individuals who believe that security measures can efficiently mitigate threats will be more inclined to actively participate in safeguarding sensitive information through security practices and measures.

Perceived Security Response Efficiency and Protective Security Intention

This hypothesis postulates that there is a substantial relationship between individuals' perception of security response efficiency and their intention to engage in protective security measures in HEIs. More specifically, it suggests that when individuals perceive security response measures as efficient and effective in addressing potential security threats, they are more likely to demonstrate a heightened intention to adopt and adhere to protective security behaviours. This hypothesis aligns with the principles of the PMT (Rogers, 1983), which propose that the perceived effectiveness of protective responses plays a pivotal role in motivating individuals to embrace such responses. In the context of information security, it is anticipated that individuals who hold the belief that security measures can efficiently mitigate threats will be more inclined to actively participate in safeguarding sensitive information through the implementation of security practices and measures.

Perceived Security Response Cost and Protective Security Intention

This hypothesis argues that there is a significant relationship between individuals' perception of security response cost and their intention to engage in protective security measures. It suggests that when individuals perceive the costs, such as time, effort, or inconvenience, associated with security responses to be low or manageable, they are more likely to exhibit a heightened intention to adopt and adhere to protective security behaviours. This hypothesis aligns with elements of the TPB (Ajzen, 2015), which emphasizes that individuals consider the perceived costs and benefits when forming behavioural intentions. In information security context, it is expected that individuals who view the costs of security measures as reasonable will be more inclined to actively participate in safeguarding sensitive information by implementing security practices and measures.

Perceived Security Efficacy and Protective Security Intention

This hypothesis posits that there is a significant relationship between individuals’ perception of security efficacy and their intention to engage in protective information security measures in HEIs. It suggests that when individuals believe that security measures are efficacious in effectively safeguarding against security threats, they are more likely to exhibit a heightened intention to adopt and adhere to protective security behaviours. This hypothesis aligns with the principles of the PMT (Rogers, 1983), which propose that the perceived efficacy of protective responses plays a crucial role in motivating individuals to embrace such responses. The hypothesis anticipates that individuals who have confidence in the effectiveness of security measures will be more inclined to actively participate in safeguarding sensitive information through the implementation of security practices and measures.

Security Attitude and Protective Security Intention

This hypothesis asserts that there exists a link between attitudes towards security and intention to engage in protective security measures. Specifically, it posits that individuals who hold positive attitudes towards security, viewing it as important and valuable, are more likely to exhibit a heightened intention to adopt and adhere to protective security behaviours. This hypothesis is rooted in the TPB (Ajzen, 2015), which emphasizes the role of attitudes in shaping behavioural intentions. In the context of information security, it is expected that individuals who have a positive outlook on security will be more inclined to actively participate in safeguarding sensitive information by implementing security practices and measures, thereby contributing to a more secure digital environment in higher education.

Subjective Security Norms and Protective Security Intention

This hypothesis posits that there is a significant relationship between subjective information security norms and intention to engage in protective security measures. It suggests that individuals who perceive a prevailing social expectation or norm that emphasizes the importance of security are more likely to exhibit a heightened intention to adopt and adhere to protective security behaviours. This hypothesis aligns with the TPB (Ajzen, 2015), which underscores the impact of subjective norms on shaping behavioural intentions. In the context of information security, it is anticipated that individuals who feel that their peers or colleagues endorse and value security will be more inclined to actively participate in safeguarding sensitive information through the implementation of security practices and measures, contributing to a culture of security in HEIs.

Concern for Securing Information Assets and Protective Security Intention

This hypothesis proposes that there is a significant and positive relationship between an individual's level of concern for securing information assets and their intention to engage in protective security measures in HEIs. It suggests that individuals who have a higher level of concern for the protection of sensitive information assets, such as student records, research data, and administrative documents, are more likely to exhibit a heightened intention to adopt and adhere to protective security behaviours. This hypothesis is grounded in the idea that heightened concern acts as a motivator for proactive security actions (Rogers, 1983). In information security context, it is expected that those who deeply concerned about safeguarding information assets will be more inclined to actively participate in the implementation of security practices and measures, contributing to a more secure digital environment in HEIs.

Proactive Security Intention and Protective Security Actions

This hypothesis assumes a significant and positive relationship between proactive security intention and engagement in protective security actions. It suggests that employees who exhibit a heightened intention to proactively participate in security measures and behaviours are more likely to take concrete protective security actions. This hypothesis is grounded in the theory that intention plays a crucial role in driving actual behaviour (Ajzen, 2015). In the context of information security, it is anticipated that individuals who genuinely intend to be proactive in safeguarding sensitive information will be more inclined to actively implement and adhere to security practices and measures, thereby contributing to a more secure digital environment within their organization or community.

Security Threat Susceptibility, Protective Security Intention and Protective Security Actions

This hypothesis proposes that protective security intention mediates the relationship between security threat susceptibility and protective security actions. It suggests that individuals who perceive themselves as more susceptible to security threats are more likely to exhibit a heightened protective security intention. In turn, this intention influences their actual engagement in protective security actions. This hypothesis is grounded in the PMT's proposition that a person's intention plays a mediating role in translating perceived threats into concrete behaviours (Rogers, 1983). Thus, it is expected that individuals who feel vulnerable to security threats are more inclined to develop a stronger intention to proactively safeguard sensitive information, ultimately leading to a greater commitment to and implementation of security practices and measures.

Security Threat Severity, Protective Security Intention and Protective Security Actions

This hypothesis suggests that protective security intention serves as a mediator in the relationship between the severity of security threats and employees' engagement in protective security actions. in other words, when individuals perceive security threats as more severe, they are more likely to develop a heightened protective security intention. Subsequently, this intention influences their actual commitment to and implementation of protective security actions. This hypothesis is grounded in the idea that individuals respond to the perceived seriousness of threats by forming intentions to protect themselves or their information assets (Rogers, 1983). Thus, it is anticipated that individuals who view security threats as highly severe will be more inclined to develop a strong intention to proactively safeguard sensitive information. This, in turn, is expected to lead to a greater commitment to and the actual implementation of security practices and measures to mitigate the perceived risks

Perceived Security Response Efficiency, Protective Security Intention and Protective Security Actions

This hypothesis proposes that protective security intention plays a crucial mediating role in the relationship between security response efficiency and protective security actions. In other words, when employees perceive security response measures as highly efficient and effective, they are more likely to develop a heightened protective security intention. This intention, in turn, influences their actual commitment to and implementation of protective security actions. This hypothesis is rooted in the idea that individuals are more inclined to act when they believe that the security response measures in place are efficient and capable of mitigating potential threats (Rogers, 1983). In the context of information security, it is expected that individuals who perceive security response measures as highly efficient will be more inclined to form a strong intention to proactively safeguard sensitive information. This intention, in turn, is anticipated to lead to a greater commitment to and the actual implementation of security practices and measures that align with their perception of security response efficiency.

Perceived Security Response Cost, Protective Security Intention and Protective Security Actions

This hypothesis posits that protective security intention acts as a crucial mediator in the relationship between individuals' perceptions of security response costs and their engagement in protective security actions. It suggests that when individuals perceive the costs associated with security responses as low or manageable, they are more likely to develop a heightened protective security intention. subsequently, this intention influences their actual commitment to and implementation of protective security actions (Rogers, 1983). In the context of information security, it is expected that individuals who perceive security response costs as low will be more inclined to form a strong intention to proactively safeguard sensitive information. This intention, in turn, is anticipated to lead to a greater commitment to and the actual implementation of security practices and measures that align with their perception of manageable security response costs.

Perceived Security Efficacy, Protective Security Intention and Protective Security Actions

In this case, it is assumed that protective security intention plays a vital mediating role in the relationship between perceptions of security efficacy and engagement in protective security actions. the hypothesis posits that when individuals perceive security measures as highly effective, they are more likely to develop a heightened protective security intention. Consequently, this intention influences their actual commitment to and implementation of protective security actions (Ajzen, 2015; Rogers, 1983). This hypothesis is based on the premise that individuals are more inclined to act when they believe that the security measures in place are effective in mitigating potential threats. In the context of information security, it is expected that employees who perceive security measures as highly efficacious will be more inclined to form a strong intention to proactively safeguard sensitive information. This intention, in turn, is anticipated to lead to a greater commitment to and the actual implementation of security practices and measures that align with their perception of security efficacy.

Security Attitude, Protective Security Intention and Protective Security Actions

This hypothesis suggests that protective security intention serves as a significant mediator in the relationship between individuals' attitudes towards security and their engagement in protective security actions. It posits that individuals who hold positive attitudes towards security, viewing it as important and valuable, are more likely to develop a heightened protective security intention. In turn, intention influences their actual commitment to and implementation of protective security actions. This hypothesis is grounded in the idea that individuals' attitudes towards security can shape their intentions and, in turn, their actual behaviours (Ajzen, 2015). In the context of information security, it is expected that individuals who have a positive outlook on security will be more inclined to form a strong intention to proactively safeguard sensitive information. This intention, in turn, is anticipated to lead to a greater commitment to and the actual implementation of security practices and measures that align with their positive security attitudes.

Subjective Security Norms, Protective Security Intention and Protective Security Actions

This hypothesis underscores the importance of individuals' perceptions regarding the costs associated with security responses in the realm of information security (Ajzen, 2015). It posits that when people view these costs as manageable or low, they are more likely to develop a strong intention to proactively safeguard sensitive information. This intention, in turn, drives them to commit to and implement protective security actions. Recognizing this mediation process is vital as it provides valuable insights for the development of effective strategies aimed at promoting information security across diverse contexts, ranging from higher education institutions to various organizations.

Concern for Securing Information Assets as Moderator Between Protective Security Intention and Protective Security Actions

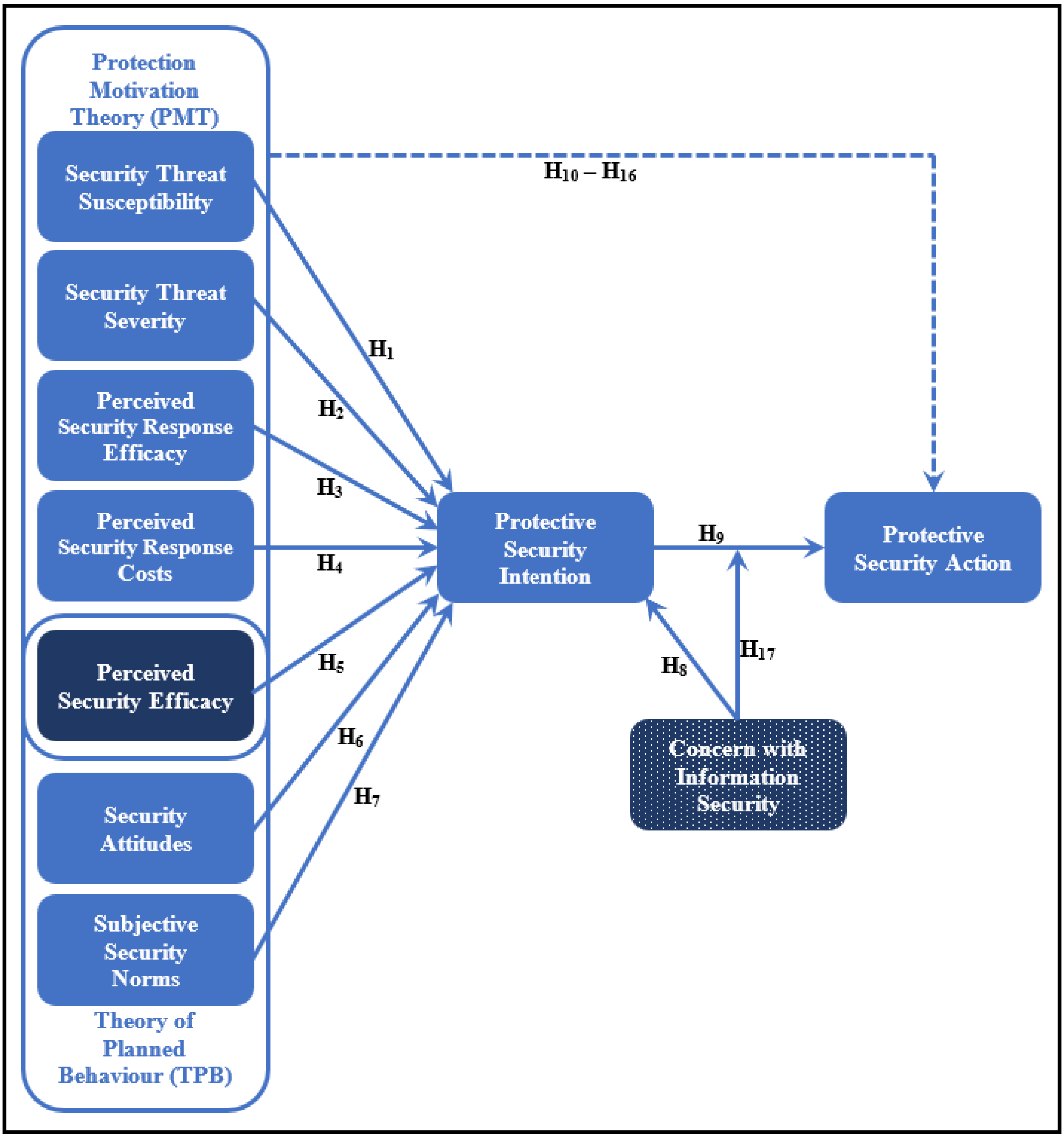
This hypothesis suggests that an individual's level of concern for securing information assets plays a crucial moderating role in the relationship between their protective security intention and their actual engagement in protective security actions. In other words, it proposes that the impact of one's intention to protect sensitive information on their subsequent security actions is influenced by the degree of concern they have for safeguarding those assets. Specifically, it posits that individuals who not only possess a strong intention to proactively secure information but also have a high level of concern for the safety of that information will exhibit a more significant commitment to and implementation of protective security actions. This hypothesis implies that concern for information security amplifies the effect of intention, reinforcing the importance of emotional and attitudinal factors in driving actual security behaviour.

Study Model

In this study, the moderated mediated was proposed. According to Preacher *et al.* (2007), a moderated mediated relationship pertains to a scenario where a fourth interacting (moderating) variable exerts an influence on an already existing mediated (or indirect) relationship that involves a minimum of three variables. Both the PMT and TPB are essentially simple mediation templates for understanding motivation and behaviour respectively. However, this study proposes to use the first issue (employee concern for securing Information Assets) both as a predictor variable extension of the PMT as well as an interacting variable (strengthening or weakening the protective security intention–protective action relationships). In other words, the proposed moderated mediation model suggests that employees' demonstration of protective actions towards institutional information assets (the desired outcome) may be driven their individual core characteristics (security threat susceptibility, security threat severity, perceived security response efficacy, perceived security response cost, perceived security efficacy, perceived security attitude, subjective security norms, and concern for securing Information Assets – predictor variables), and the effects of these predictors may be enhanced by the employees' cognitions (protective security intentions), However, the protective security intentions–protective security action relationship may be strengthened or weakened, depending on whether the employee really show concern for securing information assets or not (moderating influence). In view of these considerations as informed by the PMT (as main underpinning theory) and TPB (as a supporting theory), this study proposes to test the following model for information systems security (Figure 2.4) within the context of Nigerian HEIs.

Conclusion

This study presents an information security conceptual framework for HEIs based on two theories: PMT and TPB. It demonstrated the interaction between psychological factors, such as threat susceptibility, security efficacy, security attitude, and concern for information assets, and their influence on protective security intention, which, in turn, significantly shapes protective security actions. This framework not only underscores the importance of cultivating a culture of security within HEIs but also highlights the pivotal role of individuals' attitudes, motivations, and perceptions in driving tangible security outcomes. By harnessing these insights, institutions can tailor their strategies to enhance information security practices, ultimately fortifying their resilience against emerging threats and ensuring the safeguarding of sensitive data in an increasingly digital landscape. This research provides a foundational basis for further exploration and development of effective information security initiatives within the higher education sector, thereby contributing to the broader discourse on cybersecurity in contemporary academia.



Solid-dark box is the variable common to both PMT and TPB (Ajzen, 1991).
Patterned-dark box is an extension variable of PMT.
Figure 2.4 Model for Information Systems Security

References

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-t

Ajzen, I. (2015). The Theory of Planned Behaviour Is Alive and Well, and Not Ready to Retire: A Commentary on Sniehotta, Presseau, and Araujo-Soares. *Health Psychology Review, 9*(2), 131-137. doi:10.1080/17437199.2014.883474

Ajzen, I. and Fishbein, M. (2004). Questions Raised by a Reasoned Action Approach: Comment on Ogden (2003). *Health Psychology, 23*(4), 431-434. doi:10.1037/0278-6133.23.4.431

Al Shikhy, A., Makhbul, Z. M., Rawshdeh, Z. A., Arshad, R. and Anuar, K. (2019). Dispositional Resistance to Change and User Resistance Behaviour to Use Human Resources Information Systems in the Healthcare Sector: The Moderating Role of Conscientiousness. *International Journal of Recent Technology and Engineering (IJRTE), 8*(4), 565-572. doi:10.35940/ijrte.D7305.118419

D'Arcy, J. and Greene, G. (2014). Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance.

Information Management & Computer Security, 22(5), 474-489. doi:10.1108/imcs-08-2013-0057
Duranti, L. (2002). The Reliability and Authenticity of Electronic Records. In L. Duranti, T. Eastwood, and H. MacNeil (Eds.), *Preservation of the Integrity of Electronic Records* (pp. 23-30). Dordrecht: Springer Netherlands. doi:10.1007/978-94-015-9892-7_3.
Georg, L. (2007). *The Function of Corporate Security within Large Organisations: The Interrelationship between Information Security and Business Strategy*. (PhD Thesis), Université de Genève,
Hagen, J. M., Albrechtsen, E. and Hovden, J. (2008). Implementation and Effectiveness of Organizational Information Security Measures. *Information Management & Computer Security, 16*(4), 377-397. doi:10.1108/09685220810908796
Hanus, B. and Wu, Y. A. (2015). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16. doi:10.1080/10580530.2015.1117842
Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007
Imamov, M. M. (2018). Digital Threats in the Transition of the Russian Economy to the Innovative Path of Development. *Journal of Advanced Research in Law and Economics (JARLE), 38*, 2593-2602.
Kerlinger, F. N. and Lee, H. B. (2000). *Foundations of Behavioral Research* (Fourth edition). Fort Worth, USA: Harcourt College Publishers.
Kothe, E. J., Ling, M., North, M., Klas, A., Mullan, B. A. and Novoradovskaya, L. (2019). Protection Motivation Theory and Pro-Environmental Behaviour: A Systematic Mapping Review, Australian Journal of Psychology. *71*(4), 411-432. doi:10.1111/ajpy.12271
Larsen, K. R. and Eargle, D. (2015). Theories Used in IS Research Wiki. Retrieved from https://is.theorizeit.org/wiki/Main_Page
Lee, Y. (2011). Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective. *Decision Support Systems, 50*(2), 361-369. doi:10.1016/j.dss.2010.07.009
Liang, N., Biros, D. P. and Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems, 33*(2), 361-392. doi:10.1080/07421222.2016.1205925
Mello, S. (2018). *Data Breaches in Higher Education Institutions*. (Senior Honor's Thesis), University of New Hampshire, UK.
Meng, W., Li, W., Wang, Y. and Au, M. H. (2018). Detecting Insider Attacks in Medical Cyber–Physical Networks Based on Behavioral Profiling. *Future Generation Computer Systems*. doi:10.1016/j.future.2018.06.007
Niemimaa, E. and Niemimaa, M. (2017). Information Systems Security Policy Implementation in Practice: From Best Practices to Situated Practices. *European Journal of Information Systems, 26*(1), 1-20. doi:10.1057/s41303-016-0025-y
NIST. (2004). *Standards for Security Categorization of Federal Information and Information Systems*. Gaithersburg, MD: National Institute of Standards and Technologyb (NIST). Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
NITDA. (2019a). *Framework and Guidelines for Information and Communication Technology (ICT) Adoption in Tertiary Institutions*. Abuja, Nigeria: National Information Technology Development Agency (NITDA). Retrieved from https://nitda.gov.ng/regulations/
NITDA. (2019b). *Nigeria Data Protection Regulation 2019*. Abuja, Nigeria: National Information Technology Development Agency (NITDA) Retrieved from https://nitda.gov.ng/regulations/
Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S. and Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology, 8*(4), 1-25. doi:10.1145/2890509
Pascual, R. (2009). Enhancing Project-Oriented Learning by Joining Communities of Practice and Opening Spaces for Relatedness. *European Journal of Engineering Education, 35*(1), 3-16. doi:10.1080/03043790902989234
Preacher, K. J., Rucker, D. D. and Hayes, A. F. (2007). Addressing Moderated Mediation Hypotheses: Theory, Methods, and Prescriptions. *Multivariate Behavioral Research, 42*(1), 185-227. doi:10.1080/00273170701341316
Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology: Interdisciplinary and Applied, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803
Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. T. Cacioppo and R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). London: The Guilford Press.
Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming the "Weakest Link": A Human.Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19*(3), 122-131. doi:10.1023/a:1011902718709
Schwab, D. P. (2005). *Research Methods for Organizational Studies* (Second edition). Mahwah, New Jersey: Lawrence Erlbaum Associates, Inc., Publishers.
Sommestad, T., Karlzén, H. and Hallberg, J. (2015). The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance. *Information & Computer Security, 23*(2), 200-217. doi:10.1108/ics-04-2014-0025
Walton, R. and Limited, W.-M. (2006). Balancing the Insider and Outsider Threat. *Computer Fraud & Security, 2006*(11), 8-11. doi:10.1016/s1361-3723(06)70440-7
Wang, Y., Liang, J., Yang, J., Ma, X., Li, X., Wu, J., Yang, G., Ren, G. and Feng, Y. (2019). Analysis of the Environmental Behavior of Farmers for Non-Point Source Pollution Control and Management: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Journal of Environmental Management, 237*, 15-23. doi:10.1016/j.jenvman.2019.02.070
Warkentin, M., Johnston, A. C., Shropshire, J. and Barnett, W. D. (2016). Continuance of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems, 92*, 25-35. doi:10.1016/j.dss.2016.09.013
Winjum, E. and Mølmann, B. K. (2008). A Multidimensional Approach to Multilevel Security. *Information Management & Computer Security, 16*(5), 436-448. doi:10.1108/09685220810920521
Wood, P. (2014). Walls of Straw - the Cyber Risks to Higher Education. *Insights, 72*(2), 192-197.
Yoon, C. and Kim, H. (2013). Understanding Computer Security Behavioral Intention in the Workplace. *Information Technology & People, 26*(4), 401-419. doi:10.1108/itp-12-2012-0147
Zwanenburg, S. and Qureshi, I. (2019). Anticipating, Avoiding, and Alleviating Measurement Error: A Synthesis of the Literature with Practical Recommendations. *Australasian Journal of Information Systems, 23*, 1-21. doi:10.3127/ajis.v23i0.1844