Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior

Ali Farooq
Department of Future Technologies
University of Turku
Turku, Finland
alifar@utu.fi

Joshua Rumo A. Ndiege
Department of Computing
United States International University-Africa
Nairobi, Kenya
jrumo@usiu.ac.ke

Jouni Isoaho
Department of Future Technologies
University of Turku,
Turku, Finland
jouni.isoaho@utu.fi

***Abstract*—The purpose of this study was to identify the factors that affect the security behavior of Kenyan University Students. Using Protection Motivation Theory (PMT) and Theory and Planned Behavior (TPB) as the theoretical base, data was collected from 125 Kenyan university students through an online survey. Data Analysis was carried out using structural equational modeling (SEM) in SmartPLS 3.2. The analysis showed that among PMT constructs, only self-efficacy played a significant role towards intention to take security measures, whereas, the attitude was the only construct TPB which had a meaningful relation with behavioral intention. Lastly, out of three constructs depicting social influence, only social support had a significant relationship with the behavioral intention. Constructs such as perceived vulnerability, perceived severity, response cost, response efficacy, subjective and descriptive norms did not show a significant relationship with the security intention of the students. (*Abstract*)**

Keywords—Security behavior, protection motivation theory, theory of planned behavior, threat appraisal, coping appraisal, norms, social influence, developing countries

I. INTRODUCTION

As technological advances continue to be witnessed across the globe, so are the information technology (IT) related security threats. Such a rise is also propagated by the increase in the number of contexts in which IT is used. The contemporary educational environment continues to witness increased utilization of IT-related resources [1]–[3]. Further, it is worth noting that, today, a significant number of students are digital natives who use various electronic devices as part of their everyday life. Students' insecure security behaviors pose threats to information systems (IS) security. The IS security behaviors are not only diverse but also complex so that so it has become challenging to have a single common framework to address them [4], [5]. In the case of students, this could, among others, be attributed to the fact that the environment in which students' behaviors are exercised vary considerably [6]. Students' security behavior should be an essential research topic to IS security community. However, existing literature in security behavior has largely focused on the organizational contexts, ignoring educational environment [7]–[9]. Even more so, studies in security behavior within educational settings in developing countries is very scanty.

This paper is guided and motivated by the following argument: That there is a growing use of IT by a large population of students within universities in developing countries like Kenya. That such widespread use of IT exposes the students and their institutions even more to technology-related threats and abuses. That while studies on security behaviors of students have been carried out in universities in more developed countries [10], we know less about this subject in developing countries such as Kenya. That, the understanding of students' security behavior within Kenyan universities may prove useful in designing instructional initiatives and frameworks aimed at addressing security behavior for a more secure academic environment in developing countries, particularly Kenya.

In this study, we examined the factors that affect the security behavior of students in one of the universities in Kenya. In this regard, through a review of literature, an integrated model using the Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB) is proposed. Additionally, two constructs are added to the model for a thorough elicitation of social influence on security intention. Data was collected from 125 Kenyan university students using an online survey. The model was tested using SEM in SmartPLS 3.2.8 environment.

The rest of the paper is structured as follow: In section II, we present the theoretical background underpinning this study. Section III describes the hypotheses of the study. Research model measures and methods, and data analysis process are in Section IV. Section V describe the results, followed by discussion in section VI. The conclusion is given in Section VII.

II. THEORETICAL BACKGROUND

A. Information Security in Africa

Over the recent years, Africa has witnessed an unprecedented rise in adoption and use of technology [11]. Within the academic environment, the adoption and use of technology have increased. IT has remained the preferred choice as a tool for enhancing learning and teaching [1]–[3]. In Kenya, for instance, academic institutions continue to use IT to use blended learning as a tool to improve students' learning. To this end, the need for virtual learning environment continues to be at the centre-stage of strategic directions of academic institutions [12].

According to Africa's Cybersecurity Report released in April 2018 [13], the continent continues to witness a rise in the number and nature of cyber-attacks. Many countries in Africa, such as Kenya, are increasingly facing information security related threats and challenges. The estimated cost of cybercrime in Africa was 3.5 billion in 2017. On the other hand, the Kenya Cyber Security Report of 2018 [14], paints a picture of a country ill-prepared to tackle the growing cybersecurity challenges. The report also acknowledges the increasing use of IT within the academic environment and the

need to have policies and frameworks to deal with cybersecurity threats that are on the rise.

Although there is extensive literature on information security, there have been limited studies focusing on users' security behavior in developing countries and especially in Africa. In particular, studies on security behavior in Africa have failed to focus directly on the student population within the academic environment. In this study, we attempt to fill this gap by looking at factors affecting the security behavior of students in one of the educational institutions of higher learning in Kenya. We do this by employing the Protection Motivation Theory and Theory of Planned Behavior.

B. Protection Motivation Theory

Protection Motivation Theory (PMT) was proposed in 1974. The theory provides a theoretical framework that attempts to understand how protective behaviors are initiated [15]. This theory has been widely used to understand information security behaviors of users in different contexts when presented with several threats [16]–[18]. According to PMT theory, threat and coping appraisal motivate protective behavior. Threat appraisals are defined by the user's perceived vulnerability and severity of threats. The earlier depicts degree to which a user believes that s/he could be a victim of a threat, whereas, the latter describes the degree to which a user thinks that a threat will generate negative consequence for him/her. Self-efficacy, response efficacy, and response costs linked with safe or adaptive behaviors inform coping appraisals. Coping self-efficacy is premised on the understanding that users can positively perform protective behaviors. Response efficacy is the confidence or trust in the capability of the protections. The costs of employing security protections are considered as response costs. The coping appraisals and threat appraisals inform users' behavioral intent to adopt protections.

C. Theory of Planned Behavior

The Theory of Planned Behavior (TPB) suggests that, the intention is the driving force for a behavior, whereas, the intention is affected by three motivational factors: Attitude, subjective norms and perceived behavioral control [41]. Attitude is one's general feeling towards behavior and is also attributed as personal motivation [8]. TPB suggests that social and peer influence plays a significant role in planning behavior. In TPB, social influence is depicted by subjective norms, which is one's perception of what significant others desire from him/her to perform a specific behavior. Perceived behavioral control is similar to self-efficacy [42] and defined in the same way as in PMT(see the previous section).

D. Social Influence

Although the role of social influence in technology adoption is complex and is dependent on several influencing factors [43], it has been found that individual's behavior is influenced by the norms of the environment where they live [45]. One such construct to depict influence of the environmental norms is the subjective norm, which is part of TPB. However, the construct of subjective norm covers the *ought* (subjective) meaning of social norms, whereas, there is a long-standing debate on whether social influence includes one or both, the *is* (descriptive) and the *ought* (subjective) meanings of social influence [46]. Rivis and Sheeran [47] found that descriptive norms, referred to as one's perceptions about what most other people do, predict behavioral intention beyond social norms. In a recent study, the social norms is operationalized as the support one receives from the significant others to enact a behavior [8].

III. HYPOTHESES DEVELOPMENT

PMT model has previously been used to study the security intention and security behavior of users in both organizational and home-users' contexts. The threat appraisal has been found to predict behavioral intention in some studies, whereas no such prediction power has been found in others. Perceived vulnerability and perceived severity are a significant influencer of security intention in organizational [19]–[23] as well as in the home users context [24]–[27]. However, in certain cases, both constructs mentioned above depicting threat appraisal have been found to have either no effect [17], [28]–[30] or even negative effect [17], [31]. Studies among university students in developed countries like Australia and Korea showed that perceived severity positively affect behavioral intention to take protective actions. However, the same is not true for perceived vulnerability [32], [33]. Given the mixed findings and keeping in mind the PMT model, the following hypotheses are proposed in the Kenyan case, to examine the relationship of perceived vulnerability and severity with the security intention of Kenyan students:

H_1: *Perceived vulnerability will positively affect the security intention of Kenyan students*

H_2: *Perceived severity will positively affect the security intention of Kenyan students*

Coping appraisal in PMT is depicted by response cost and response efficacy. Response cost is not just the financial cost but includes other resources such as time, effort and inconvenience that a user invests for a security behavior. Considering that perceived cost is context dependent construct, its influence on behavioral intention may vary across different contexts. For example, in the home users context, the perceived cost has been found to affect security intention negatively[24], [27], [28], [34]. However, no significant relationship was found between the same constructs in studies conducted in organizational context [19], [35]. Like home users, the studies conducted on students' security behavior suggest a significant negative relationship between response cost and behavioral intention. To ascertain if response cost has a significant role to play in Kenyan students' behavioral intention, we propose the following hypothesis:

H_3: *Response cost will negatively affect security intention of Kenyan students*

In the existing studies, the significant influence of self-efficacy and response efficacy with security intention has been reported in both organizational [19], [20], [23], [36], [37] and home-users contexts [28], [30], [35], [36], [38], [39]. In a recent study [27], a significant positive influence of self-efficacy on security intention in the context of home computers and mobile devices was found. However, no significant relationship of response-efficacy with security intention was found in the same study [27]. In other studies, an insignificant relationship between self-efficacy and security intention has also been reported [17], [40]. With this background, the following hypotheses are proposed to examine the relationship of response efficacy and self-efficacy with the behavioral intention of Kenyan students:

H4: *Response efficacy will positively affect the security intention of Kenyan students*

H5: *Self-efficacy will positively affect the security intention of Kenyan students*

The role of behavioral control (also known as self-efficacy) is like self-efficacy in PMT model, and the corresponding hypothesis has been discussed above.

The relationship between attitude and behavioral intention has been studied in several studies in information systems literature [43]. Most of the studies focus on attitude-behavioral intention relationship and are conducted in organizational context. There are several studies that shows a positive association of attitude towards security, and behavioral intention (For example, [19], [20], [44]). Similar findings have been reported in home-users context as well; that attitude is a significant predictor of precautionary behavioral intention [39]. Following hypothesis is proposed for studying the relationship of security attitude and security intention of Kenyan students:

H6: *Security Attitude will have a positive effect on the security intention of Kenyan students*

The third construct of TPB is subjective norms. Ifinedo [19] while studying employee compliance towards security policy, found that social influence plays a vital role in creating an environment where employees follow security policies. Subjective norms are used to study social influence in the study mentioned above. In another study [48], both subjective and descriptive norms were used to study the social influence on performing security-related measures on home computers and with regards to internet use. The result from this study showed that subjective norm was influential in implementing security measures on home computers, but the same was not right for intention to take steps for online security. The reverse was true for descriptive norms. In the home user's context, there are mixed findings. For example, one study shows that descriptive norms significantly influence security intention but subjective norms have not a significant relationship with security intention [27]. Another indicates that subjective norms significantly predict security intention among home users[30]. In studies related to students, subjective norms were not found to play a significant role either [33]. A recent research [8] shows social support does not significantly relate to actual security behavior, however, no study has been carried out to examine the relationship of social support and security intention. Following hypotheses are suggested to discussed the role of social influence on security intention of Kenyan students:

H7: *Subjective norms will positively affect the security intention of Kenyan students*

H8: *Descriptive norms will positively affect the security intention of Kenyan students*

H9: *Social support will positively affect the security intention of Kenyan students*

A. Security Intention and Actual Behavior

Most of the previous security research, where PMT and TPB have been used, is based on the intention-based model. While there is debate if security intention transforms to actual security behavior, there is evidence that behavior does follow the intention [49]. Even PMT and TPB have the same premise. In an organizational context, a study showed that the intention has a stronger influence on actual behavior to comply with policies [21]. Similar findings have been reported in home-users settings as well [24], [27], [50]. To examine if security intention does predict security behavior among the Kenyan students, we proposed the following hypothesis:

H10: *Security intention will positively affect the security behavior of Kenyan students*

IV. Research Methodology

A. Research Model

Based on the discussion in section III, the research model for the study is presented in Figure 1. The proposed model is a combination of PMT, TPB theory, and additional constructs for social influence. Between PMT and TPB, there are is one common construct, *self-efficacy*. Whereas, social influence is depicted by the *descriptive norms* and *social support*, in addition to *subjective norm*, a construct of TPB. The dependent variable is the *security behavior*.

B. Questionnaire and Procedure

Data was collected using an online survey designed in English using an online tool called Webropol. The questionnaire started with an introductory page, followed by seeking the explicit consent of the participants. Items related to different constructs shown in Figure 1 were presented to participants on separate pages/sections in the following order: threat appraisal, coping appraisal, social influence including subjective norm, descriptive norm and social support, attitude and behavioral intention, security behavior, and lastly items related to demographic information. Items on each page were presented randomly to the participants. Also, two attention check items were added to check due diligence of the participants. The participants for the study were recruited from a private university in Kenya and data collection was carried out in June-July 2018. In this way, a total of 123 responses were collected, of which none failed the attention check criteria.

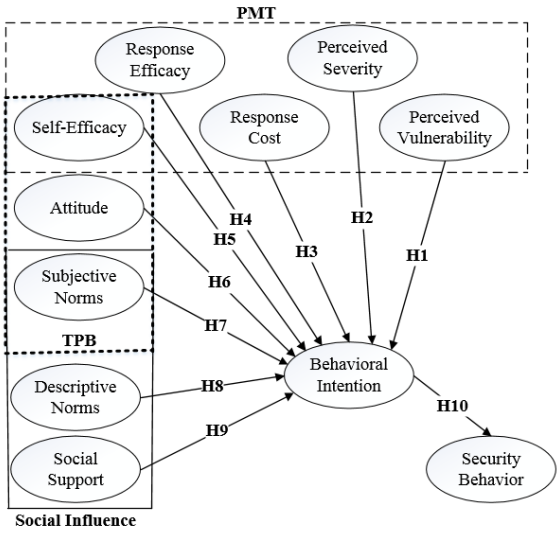

Fig. 1. Research Model consisting of PMT, TPB, and social influence construct

C. Measures

Altogether, there were 11 constructs, nine independent, one intermediate and one dependent. All the constructs, except *security behavior*, were measured using 7-point Likert scale

items (1=strongly disagree to 7=strongly agree). *Security* behavior was measured on a 5-point scale (1 =never, 2=rarely, 3=sometimes, 4=often, 5=always). All the theory related construct except for *security behavior* were reflective. Items in reflective constructs show a common cause where cause flows from constructs to items, whereas, formative constructs are a composite measure summarizing a common variation through a set of items. The causal relationship in the formative construct flows from items to the construct (for further differences refer to [51]). According to Chin [51], in the formative construct, the removal of a single item can affect the construct negatively. Considering the guidelines provided by [52], and that users have to take more than one measures to avoid a threat or minimize risks, we decided to use our dependent variable, security behavior as a formative construct. Farooq et al. also used a formative measure for security behavior for testing the information-motivation-behavioral skills model [8].

Table I describes the initial number of items used to measure a construct, sample item, along with sources from where the items were adapted. The full questionnaire is available on request from the corresponding author.

TABLE I. CONSTRUCTS DETAIL WITH SOURCES

Construct	Sample Item	Source(s)
Perceived Vulnerability (6)	I could be subject to a serious information security threat.	[19], [21], [27], [28]
Perceived Severity (6)	An information security breach on my system/accounts would be a serious problem for me.	[19], [21], [22], [27]
Response Cost (5)	Implementing security measures would be time-consuming.	[22], [28], [53]
Response Efficacy (4)	Enabling security measures will prevent security breaches	[27], [28]
Self-Efficacy (6)	I feel comfortable taking measures to secure my information security.	[27], [48]
Attitude (4)	I am likely to take security measures for my information security.	[8], [54]
Subjective Norm (3)	Significant others who are important to me think that I should take measures for my information security.	[54], [55]
Descriptive Norm (4)	I believe other people implement security measures.	[48], [55]
Social Support (3)	Significant others who are important to me introduce me to the measures for my information security.	[8]
Behavioral Intention (4)	I intend to take measures to protect my information security	[27], [54]
Security Behavior (12)	I use different passwords for different accounts	[8]

In addition to above, the questionnaire also captured demographic information, such as gender, age, education level and discipline, previous information security related training, internet experience and the device they use mostly to access the internet. Measurement scales for these items can be seen in the Result section.

D. Data Analysis

Considering the complexity of the model, small sample size, and non-normally distribution of data, Partial Least Square Structural Equation Modeling (PLS-SEM) was in SmartPLS 3.2 environment [56]–[58]. In PLS-SEM, the model is tested in two phases: 1) testing of the measurement model, and 2) testing of the structural model. In both steps, we used established guidelines [57], [59], [60].

1) Measurement model-Reflective Constructs

All the dependent constructs and *behavioral intention* were reflective. For reliability of constructs, internal consistency was checked with the help of composite reliability (CR), and items reliability was tested through item loadings [57]. CR is considered a more suitable measure of reliability in PLS than Cronbach alpha [61]. The validity of the construct was tested using convergent validity and discriminant validity. Convergent validity was measured with the help of average variance explained (AVE) [57], and Fornell-Larcker criterion was used for the latter [62].

First run of reliability and validity testing showed that six dependent constructs (*perceived vulnerability, perceived severity, descriptive norm, subjective norm, social support and behavioral intention*) had CR, item loadings, and AVE above the recommended threshold (CR>0.70, item loadings >0.70, and AVE>0.50) [57]. However, three dependent constructs (*response cost, response efficacy, self-efficacy* and *attitude)* could not pass one or more of above-stated thresholds. So, we dropped the items which were loading <0.70 on a given construct, we brought the values for CR, item loadings, and AVE above the recommended threshold. In this process, we dropped three items each from *response cost* and *self-efficacy*, one from *response* efficacy, and two from *attitude*.

For assessment of discriminant validity, Fornell-Larcker criterion was used. The average variance extracted from each construct was compared with the correlation among the constructs [63]. Table II shows the final number of items used in the structural model testing, Mean and standard deviation (SD), items loading range, CR, AVE, correlation coefficients and the square roots of each construct's AVE, along the diagonal.

2) Measurement model-Formative Construct

The quality of formative construct, s*ecurity behavior* was assessed through collinearity diagnosis and significance of the formative items, for which guidelines recommended by Hair Jr et al. [57] were followed. Variance inflation factor (VIF) of all formative items was between 1.4 and 2.06, which was between the recommended threshold (0.2–5) [57]. The significance of formative items was assessed in two steps. First, we checked the significance of outer weights; if the outer weights were not significant, out-loadings were checked. The items having outer-loadings > 0.5 were retained, even if the outer weights were insignificant. For items having outer-loadings <0.5, the significance of outer-loading was checked. If the outer-loading was significant ($p<0.05$), item was retained otherwise dropped from further analysis [57]. Following these guidelines, two out of 12 items could not pass the significance test and were thus removed from further analysis.

V. RESULTS

A. Participants

The study participants were asked to elicit their gender by selecting one of the following options: male, female, prefer not to tell. Out of 123 respondents, 69% were male, 31% were female. 89% of respondents were bachelor level students while the rest were taking one of a master level program. The average age of participants was 22.34 (SD = 3.99) with a range of 17-35. The respondents had their ages in years.

TABLE II. MEASUREMENT MODEL STATISTICS – COMPOSITE RELIABILITY, AVE AND DISCRIMINANT VALIDITY OF REFLECTIVE CONSTRUCTS

S#	Constructs (Final # of items)	M(SD)	Loading Range[a]	CR[a]	AVE[a]	Discriminant Validity (Fornell-Larcker Criterion)[a]									
						1	2	3	4	5	6	7	8	9	10
1	Attitude (2)	4.97(1.36)	0.72-0.79	0.88	0.57	**0.90**									
2	Behavioral Intention (4)	6.20(1.23)	0.78-0.90	0.94	0.73	0.80	**0.89**								
3	Descriptive Norm (3)	3.90(1.50)	0.74-0.78	0.74	0.59	0.23	0.28	**0.79**							
4	Perceived Severity (6)	5.39(1.31)	0.81-0.83	0.89	0.72	0.33	0.43	0.11	**0.85**						
5	Perceived Vulnerability (6)	5.13(1.31)	0.71-0.84	0.83	0.63	0.27	0.31	0.12	0.61	**0.75**					
6	Response Cost (2)	6.23(1.10)	0.89-0.91	0.89	0.81	-0.09	-0.14	0.28	-0.17	0.02	**0.77**				
7	Response Efficacy (3)	4.45(1.34)	0.81-0.83	0.86	0.68	0.43	0.48	0.34	0.42	0.38	0.10	**0.85**			
8	Self-Efficacy (3)	4.53(1.33)	0.73-0.89	0.87	0.63	0.45	0.63	0.30	0.40	0.37	-0.01	0.57	**0.79**		
9	Ssubjective Norm (3)	4.19(1.37)	0.71-0.88	0.85	0.67	0.19	0.24	0.47	0.08	0.18	0.21	0.24	0.31	**0.82**	
10	Social support (3)	6.01(1.09)	0.88-0.90	0.94	0.76	0.17	0.32	0.49	0.089	0.19	0.18	0.27	0.38	0.61	**0.81**

[a.] Acceptable thresholds: Item loading >0.70, CR>0.70, AVE>0.5 [57]. Discriminant validity is tested by comparing the square root of each construct's AVE with the correction among each construct.

About one-third of respondents were computer science and information technology student (77%) while the rest were from other disciplines. Options available to respondents were: business & economics, humanities, information technology, engineering, computer science, other natural sciences, law, and social science. About half of them (47%) had an information security-related training previously.

Respondents internet experience was measured using two items: 1) measuring internet use in terms of time/ per day where they could select one of the following options (in hours): 1-3, 3-5, 5-8, 8-10 and more than 10; 2) measuring internet experience in years. 83% of the respondents use the internet for up to 10 hours in a day, with the majority using for 5 to 8 hours (30%). On average, a respondent has been using the internet for 10.69 years (SD = 1.88) with a range of 0-20. In terms of the preferable device to access/use the internet, 57% prefer their mobile phones to use the internet, while 30% use the internet on laptops or computers running the Windows operating system. The rest use other devices such as laptops/computers running other type of operating systems.

B. Hypothesis Testing

The main purpose of the study was to analyze the factors that affect the security behavior of the respondents and to suggest ways to improve their security behavior. The standardized path coefficients (β), the coefficient of determination (R^2), and significance (at $p<0.05$) for each relationship is shown in Figure 2.

Next, we describe results of measurement model testing for each construct one by one, starting with constructs of PMT followed by TPB and social influence. Lastly, the relationship between behavioral intention and actual behavior is discussed.

1) PMT Constructs

Threat appraisal in PMT consists of two constructs, perceived *vulnerability and* perceived *severity. As shown in Figure 2, no significant relationship was found between* perceived vulnerability and behavioral intention (β = -0.05, p = 0.39), and perceived severity and behavioral intention (β = 0.12, p = 0.07). Thus, our hypotheses H_1 and H_2 were not supported. Further, the constructs of threat appraisal did not have a significant indirect effect on security behavior either.

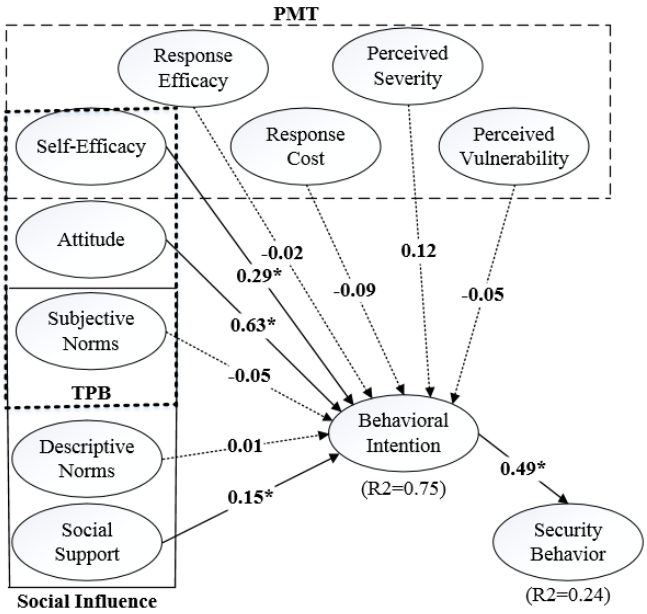

Fig. 2. Research Model with path coefficients (β) and determination coefficients (R^2). * and dark arrows depict significant relationship (at $p<0.05$); dotted arrows show an insignificant relationship between the constructs.

Coping appraisal of PMT consist of three constructs: *response cost, response efficacy* and *self-efficacy*. Of these three constructs, only *self-efficacy* had a significant relationship with *behavioral intention* (β = 0.29, $p < 0.01$).

Response cost (β = -0.08, p = 0.08) and *response efficacy* (β = -0.02, p = 0.74) had insignificant relationship with *behavioral intention*. Thus, our data provided did not support hypotheses H_3 and H_4 but supports only H_5. Further, *self-efficacy* found to have a significant indirect effect on *security behavior* as well (t=2.88, $p <0.01$).

2) TPB Constructs

TPB model has three dependent constructs: *self-efficacy, attitude* and *subjective norm*. The relationship of *self-efficacy* with *behavioral intention* and *security behavior* has already been discussed in the previous section.

Attitude towards information security, which is also called intrinsic motivation was found to have significant relationship with *behavioral intention* ($\beta = 0.63$, $p < 0.01$), whereas, the construct of TPB depicting social influence, *subjective norm* did not have a significant relationship with *behavioral intention* ($\beta = -0.05$, $p = 0.42$). This implies that H_6 was supported, but H_7 was not. Further, the *attitude* was found to have a significant indirect effect on *security behavior* as well (at $p < 0.01$).

3) Social Influence

Originally, social influence in TPB was measured using *subjective norm*, however, as mentioned in section II, to understand the effect of social influence, we used *descriptive* norm and *social support* as an additional construct to depict social influence. Through analysis and as shown in Fig 2, *descriptive norm* did not have a significant relationship with *behavioral intention* ($\beta = 0.01$, $p = 0.81$), whereas, *social support* predicted *behavioral* significantly ($\beta = 0.15$, $p = 0.02$). Thus, our hypothesis H_8 was not supported, however, H_9 was supported. Further, social support was found to have significant indirect effect on *security behavior* as well (at $p = 0.02$).

4) Behavioral Intention and Security Behavior

Finally, our hypothesis H_{10} that there was a significant relationship between *behavioral intention* and actual *security behavior* was also supported. There was a significant relationship found between *behavioral intention* and *security behavior* ($\beta = 0.49$, $p < 0.01$).

VI. Discussion

PMT and TPB have been used in users' security behavior related research in both organizational and home-users context, mostly in advanced countries. We have used an integrated model consisting of PMT and TPB constructs (with additional constructs for social influence), to understand the factors that affect the security behavior of students from a developing country.

Among PMT constructs, only self-efficacy was the significant predictor of the behavioral intention of the students. This result is consistent with findings from other studies conducted in organizational [19], [36] and home-users domains [24], [28], [30], [34]. At the same time, the relationship of response efficacy and response cost with behavioral intention was insignificant. The insignificant relationship between response efficacy and the behavioral intention was surprising as most of the previous studies showed evidence of significant relationship [28], [30], [32], [33], [35], [39]. However, a study on home-users on device security [27] showed similar results for response efficacy. The insignificance maybe because we asked students about a range of common security behavior. A meta-analysis of PMT [18] showed that the relationship between response efficacy and the intention was salient in specific behaviors than the general behaviors, The third construct related to coping appraisal was response cost, which should be related with intention negatively (as postulated by the PMT). However, in our study, contrary to our expectation, we did not find this relationship meaningful either. This result is in line with results from earlier studies conducted in organizational [19] or home settings [30], [35].

Like response cost, and response efficacy constructs of coping appraisal, both constructs of threat appraisal of PMT, neither perceived vulnerability nor perceived severity, show a significant relationship with intention. This finding was also surprising as it defies the main contention of PMT that if a person can appraise a threat, s/he will intend to take precautionary actions for his/her security. Previous studies, both in organizational and home settings, have provided evidence of a significant relationship of threat appraisal constructs with the intention (For example, [19], [23], [32], [33], [36], [39]). However, a few studies, such as [27], [30], found similar results while studying home users computer-related security behaviors in home-settings. Our findings may be because of the reason that our student sample may not have higher threat appeal. A previous study showed that lower threat appeal had less impact on behavioral intention of the respondents [36]. Another possible explanation for this different outcome could be because respondents were asked about perceived severity and perceived vulnerability in general. A specific threat and behavior could produce a significant relationship.

In addition to studying the relationship of PMT constructs, we also examined the relationship of TPB constructs. Out of three TPB constructs, attitude, self-efficacy and subjective norms, two had a significant association with intention. The relationship of self-efficacy has already been described, whereas attitude was the other factor that significantly predicted the intention of Kenyan students. Attitude has been the strongest predictor for the intention in our study, which is in line with findings from earlier studies [39], [43], [48], [64]. In TPB, subjective norms are used to depict social influence, and it was expected that subjective norms would influence the behavioral intention of the students. However, we could not find a significant relationship between subjective norms and behavioral intention.

To have a holistic understanding of the social influence on students' intention to take security measures, we used two additional constructs, descriptive norms and social support. Out of three constructs for social influence, social support was the only construct that showed a significant effect on intention, other two (subjective norms and descriptive norms) did not have a significant relationship with the intention. This insignificant relationship of subjective norms has been found in earlier studies on home users as well [27], [39]. One possible explanation of the lack of influence of subjective norms could be that students are not sure about what significant others want them to do. In organizational contexts, the relationship of subjective norms can be more salient as the significant others can be the managers, thus having a stronger effect than our case. Like subjective norms, the relationship of descriptive norms, which is the perception of what significant others do, with intention was insignificant. This result was in contradiction to earlier findings where descriptive norms significantly predicted behavioral intention of the users [27], [39]. One possible reason could be that students are not sure what other students do in the face of information security threat. From above, we can also say that students were unclear about what their peers do for their information security and that what are their obligations towards others when it comes to information security practices. Lastly, we found that social support had a significant relationship with behavioral intention. In an earlier study [8], the relationship of social support and actual security behavior was insignificant, however, in our case, the relationship of social support and the behavioral intention was significant. It means that students expect family, peers and friends to support them to improve

their security behavior. We did not ask specifically about the support provided by the educational institutions, but it will be interesting to examine if the support provided by the educational institution will influence the behavioral intention of the students.

VII. Conclusion

The purpose of this study was to examine the factors that affect the security behavior of Kenyan university students. In this regard, from the literature review, an integrated model, consisting of constructs from the Protection Motivation Theory and the Theory of Planned Behavior was proposed. Using an online survey data was collected from 125 Kenyan university students. Data analysis was conducted using structural equation modeling in SmartPLS 3.2. The results show that attitude is the strongest predictor of the behavioral intension among the students. Among others, self-efficacy and social support were significant predictors of the behavioral intention related to information security. Constructs related to threat appraisal, and norms did not show significant influence on the intention. Lastly, a significant relationship between behavioral intention and behavior was also found.

References

[1] F. AlTameemy, "Mobile Phones for Teaching and Learning: Implementation and Students' and Teachers' Attitude," *J. Educ. Technol. Syst.*, vol. 45, no. 3, pp. 436–451, Mar. 2017.

[2] S. Assar, R. El Amrani, and R. T. Watson, "ICT and education : a critical role in human and social development," *Inf. Technol. Dev.*, vol. 16, no. 3, pp. 151–158, 2010.

[3] M. M. Chingos, R. J. Griffiths, C. Mulhern, and R. R. Spies, "Interactive Online Learning on Campus: Comparing Students' Outcomes in Hybrid and Traditional Courses in the University System of Maryland," *J. Higher Educ.*, vol. 88, no. 2, pp. 210–233, Mar. 2017.

[4] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," *J. Inf. Secur. Appl.*, vol. 44, pp. 12–22, Feb. 2019.

[5] S. Furnell, V. Tsaganidi, and A. Phippen, "Security beliefs and barriers for novice Internet users," *Comput. Secur.*, vol. 27, no. 7–8, pp. 235–240, Dec. 2008.

[6] R. Wash and E. Rader, "Too Much Knowledge? Security Beliefs and Proactive Behaviors Among United States Internet Users," in *SOUPS*, 2015, pp. 309–325.

[7] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, "Factors that Influence Information Security Behavior: An Australian Web-Based Study," in *Human Aspects of Information Security, Privacy, and Trust*, Springer, Cham, 2015, pp. 231–241.

[8] A. Farooq, D. Jeske, and J. Isoaho, "Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model," in *34th International Conference on ICT Systems Security and Privacy Protection*, 2019.

[9] A. Farooq, J. J. Isoaho, S. Virtanen, and J. J. Isoaho, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, pp. 352–359.

[10] R. Alomari and J. Thorpe, "On password behaviours and attitudes in different populations," *J. Inf. Secur. Appl.*, vol. 45, pp. 79–89, Apr. 2019.

[11] E. T. Lwoga and R. Z. Sangeda, "ICTs and development in developing countries: A systematic review of reviews," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 85, no. 1, p. e12060, Jan. 2019.

[12] D. N. Mutisya and G. L. Makokha, "Challenges affecting adoption of e-learning in public universities in Kenya," *E-Learning Digit. Media*, vol. 13, no. 3–4, pp. 140–157, May 2016.

[13] Serianu, "Africa Cyber Security Report 2017," 2017.

[14] Serianu, "Kenya Cyber Security Report," 2018.

[15] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975.

[16] S. F. Verkijika, "Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret," *Comput. Secur.*, vol. 77, pp. 860–870, Aug. 2018.

[17] H. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput. Secur.*, vol. 59, pp. 138–150, Jun. 2016.

[18] T. Sommestad, H. Karlzén, and J. Hallberg, "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *Int. J. Inf. Secur. Priv.*, vol. 9, no. 1, 2015.

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

[20] B. Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, Mar. 2009.

[21] M. Siponen, A. Mahmood, and S. Pahnila, "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, Mar. 2014.

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

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

[24] H. Liang and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010.

[25] T. Chenoweth, R. Minch, and T. Gattiker, "Application of Protection Motivation Theory to Adoption of Protective Technologies," in *42nd Hawaii International Conference on System Sciences*, 2009, pp. 1–10.

[26] C. L. Claar and J. Johnson, "Analyzing Home PC Security Adoption Behavior," *J. Comput. Inf. Syst.*, vol. 52, no. 4, pp. 20–09, 2012.

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

[28] I. Woon, G.-W. Tan, R. Low, I. M. Y. Woon, G. W. Tan, and R. T. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in *International Conference on Information Systems (ICIS)*, 2005.

[29] L. Zhang and W. C. McDowell, "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *J. Internet Commer.*, vol. 8, no. 3–4, pp. 180–197, Dec. 2009.

[30] A. M. Mills and N. Sahi, "An Empirical Study of Home User Intentions towards Computer Security," in *Proceedings of 52nd Hawaii International Conference on System Sciences*, 2019, pp. 4864–4840.

[31] R. E. Crossler, "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–10.

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

[33] C. Yoon, J.-W. J.-W. Hwang, and R. Kim, "Exploring Factors that Influence Students' behaviors in Information Security," *J. Inf. Syst. Educ.*, vol. 23, no. 4, pp. 407–415, 2012.

[34] F. Mwagwabi, T. McGill, and M. Dixon, "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines," in *47th Hawaii International Conference on System Sciences (HICSS)*, 2014, pp. 3188–3197.

[35] P. Menard, G. J. Bott, and R. E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *J. Manag. Inf. Syst.*, vol. 34, no. 4, pp. 1203–1230, Oct. 2017.

[36] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Q.*, vol. 39, no. 4, pp. 837–864, 2015.

[37] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Inf. Syst. J.*, vol. 24, no. 1, pp. 61–84, Jan. 2014.

[38] R. LaRose, N. J. Rifon, and R. Enbody, "Promoting personal responsibility for internet safety," *Commun. ACM*, vol. 51, no. 3, pp. 71–76, Mar. 2008.

[39] J. Jansen and P. van Schaik, "Comparing three models to explain precautionary online behavioural intentions," *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 165–180, Jun. 2017.

[40] D. Dang-Pham, S. Pittayachawan, and V. Bruno, "Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace," *Comput. Human Behav.*, vol. 67, pp. 196–206, Feb. 2017.

[41] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991.

[42] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice-Hall, Inc, 1986.

[43] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Q.*, vol. 27, no. 3, p. 425, 2003.

[44] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, pp. 523–548, 2010.

[45] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[46] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, May 2009.

[47] A. Rivis and P. Sheeran, "Descriptive norms as an additional predictor in the theory of planned behaviour: A meta-analysis," *Curr. Psychol.*, vol. 22, no. 3, pp. 218–233, Sep. 2003.

[48] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Q.*, vol. 34, pp. 613–643, 2010.

[49] S. Egelman, M. Harbach, and E. Peer, "Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS)," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 2016, pp. 5257–5261.

[50] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, Mar. 2015.

[51] W. W. Chin, "The partial least squares approach to structural equation modeling," in *Modern methods for business research*, George A. Marcoulides, Ed. 1998, pp. 295–336.

[52] C. B. Jarvis, S. B. MacKenzie, and P. M. Podsakoff, "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *J. Consum. Res.*, vol. 30, no. 2, pp. 199–218, Sep. 2003.

[53] T. & Mcgill, H. Australia, N. Thompson, and T. Mcgill, "Australasian Conference on Information Systems Mining the Mind – Applying Quantitative Techniques to Understand Mental Models of Security Australasian Conference on Information Systems," in *Australasian Conference on Information Systems*, 2017.

[54] S. Taylor and P. A. Todd, "Understanding Information Technology Usage: A Test of Competing Models," *Inf. Syst. Res.*, vol. 6, no. 2, pp. 144–176, Jun. 1995.

[55] E. Ernovianti *et al.*, "The Usage of Internet Banking Service among Higher Learning Students in Malaysia," *Am. J. Econ.*, no. June, pp. 105–108, 2012.

[56] C. M. Ringle, D. Smith, and R. Reams, "Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers," *J. Fam. Bus. Strateg.*, vol. 5, no. 1, pp. 105–115, Mar. 2014.

[57] J. F. Hair Jr, G. T. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publishers, 2016.

[58] P. B. Lowry and J. Gaskin, "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It," *IEEE Trans. Prof. Commun.*, vol. 57, no. 2, pp. 123–146, Jun. 2014.

[59] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate data analysis*, 7th ed. Prentice Hall, Upper Saddle River, NJ, 2010.

[60] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, Jan. 2015.

[61] J. Henseler, C. M. Ringle, and R. R. Sinkovics, "New Challenges to International Marketing The use of partial least squares path modeling in international marketing," *New Challenges to Int. Mark.*, pp. 277–319, 2015.

[62] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J. Mark. Res.*, vol. 18, no. 1, p. 39, Feb. 1981.

[63] K. K. K. Wong, "Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS," *Mark. Bull. Tech. Note*, vol. 24, no. 1, 2013.

[64] M. Fishbein and I. Ajzen, *Predicting and Changing Behavior: The Reasoned Action Approach*. New York: Taylor and Francis, 2010.