International Journal of Engineering

Journal Homepage: www.ije.ir

Effect of motivation, opportunity and ability on human resources information security management considering the roles of Attitudinal, behavioral and organizational factors

Leila Bahrami[1], Nasser Safaie[1]*, Hojatollah Hamidi[2]

[1] *Faculty of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran*
[2] *Department of Information Technology, Faculty of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran*

PAPER INFO

Paper history:
Received 10 July 2021
Received in revised form 26 August 2021
Accepted 30 August 2021

Keywords:
Information security
Human resources behavior
Motivation Opportunity Abbility model
Norm Activation Model
Planned Behavior theory

ABSTRACT

Information security is a vital issue currently faced by organizations around the world. There is a huge flood of cyber-attacks and security threats due to the negligence of human agents, which doubles the importance of human resource behavior in the organization. This study provides an integrated framework of motivation opportunity-ability (MOA) that includes social psychological factors from the norm activation model (NAM) model and planned behavior (PB) theory to examine the variables that determine security behaviors in a well-founded university in Tehran. For this purpose, data were collected and analyzed by distributing 141 questionnaires among the staff of this university. The research hypotheses have been tested by structural equation modeling (SEM) using SPSS and Lisrel software. The results show that the ability has the greatest impact on information security behaviors, followed by opportunity and motivation, which have a direct and significant impact on behavior. In addition, motivation mediates the impact of opportunity and ability. Finally, recommendations are provided for designers of effective information security strategies based on the constraining factors of human resources behavior in the organization.

doi: *10.5829/ije.2021.34.12C.07*

1. INTRODUCTION

Today, Modern organizations have broad range of information resources that are heavily dependent on their human resources factors, and this dependency has made them vulnerable to events that could jeopardize their information systems [1]. Information leakage has serious consequences for organizations, including reputation damages, loss of intellectual property, reduced productivity, loss of competitive advantage, and, worst of all, and bankruptcy. In another words, organizations have identified people as a significant liability to information security governance [2], security and risk, economics and technology, which is among the industries rapidly growing and developing [3]. Therefore, the role of information security is essential in organizations to protect data and ensure that services and projects are categorized and successfully performed without disclosing information [4] and which has become an overwhelming challenge [5].

Evidence shows that the number and severity of information security breaches is increasing and has been a major concern for users and organizations. According to Karjalainen et al. [6], the average cost of cybercrime has increased by 62% over the past 5 years. Lloyd's, the British insurance company, stated in a report that its annual loss would be $ 400 billion in the absence of cybersecurity mechanisms [7]. DBIR Research Center claims that occurrence of 60% of information security threats can seriously endanger organizations within minutes. In this report, 55% of information security incidents are the result of the workings of human resources inside organizations [8]. The IBM Cyber Security Information Index also reported that 95% of information security incidents were related to human error [9].

* Corresponding Author Institutional Email: nsafaie@kntu.ac.ir (N. Safaie).

Please cite this article as: L. Bahrami, N. Safaie, H. Hamidi, Title must be Cambria 8, International Journal of Engineering, Transactions C: Aspects Vol. 34, No. 12, (2021),

Intentionally or unintentionally, employees make up a significant portion of threats to organizations' information assets. According to the findings and after analyzing two case studies, public and private sector organizations participating in these studies stated that 92.5% and 51% of the recorded information security incidents have been related to human error, respectively [10]. According to a research report by the Ponemon Institute on the cost of cyber security attacks, internal threats are of the highest costs, the impact of which is not limited to financial losses, but may also endanger the security of individuals and the organization [11]. In the literature, several theories postulated after investigations by researchers and reported human factors to have had an impact on user behavior, both negative and positive which is mentioned by researchers and security experts have reported that the "weakest link" in any security chain is human behavior; because any technical security solution is still prone to failures due to human error [12]. From a practical perspective, understanding such behaviors is important; if users do not comply with information security solutions; however, technically sophisticated, lose their effectiveness [13]. Therefore, it is recognized that in the field of information security, reducing the risk requires attention to human aspects along with technological aspects. Domestic staff does not require much effort and time to access targeted information compared to foreign attackers. Organizations often trust their employees, and anonymity is a feature that can reduce the risk of identifying them. Due to their constant involvement with highly complex security systems and a wide range of other job requirements, domestic staff may easily ignore unlikely information security threats or take no action on them, because they neither have the time, nor do they have enough skills to respond to these threats. As a result, the potential harms of domestic staff are increasing.

In order to understand the main factors of human resources security behaviors in organizations, the question of the present study is as follows: What are the determinants of human resources security behaviors in the field of organizational information? The results of this study can be effective in improving the information security behaviors of human resources of organizations by helping managers apply appropriate strategies in accordance with the characteristics of employees. In the following, while reviewing the background of the studies, the theoretical foundations, conceptual model and also the research method are provided. The results are analyzed in a well-founded university in Tehran and finally, the conclusion and key factors affecting the information security of human resources in the organization are presented.

Therefore, according to experts, the "weakest link" in any security chain is human behavior because any technical security solution is still subject to failures resulting from human errors. Hence, the risk reduction in information security area involves paying attention to aspects of human being along with technological aspects. As a result, one of the main motives of this study is investigating the factors affecting the security behaviors of human resources in the organization. the purpose of this study is to determine the relationship between attitudinal, behavioral and organizational factors with empirical support from three theoretical frameworks including Theory of planned behavior, the norm activation model (NAM) and motivation model with the interdisciplinary approach, in the integration form.

The structure of this paper consists of follow sections; in the second section, the literature of the research is reviewed and in the third section, the research model and hypotheses are presented. Section forth provides research method and results, and section fifth devoted to findings and conclusions. In the final section, limitations of the research and suggestions for future research are presented.

2. LITERATURE REVIEW

2.1. Norm Activation Model (NAM)

The NAM theory, first developed by Schwartz [14], is a social-friendly theory to explain the purpose of humanitarian behaviors. The theory states that personal norms are an essential prerequisite for each individual's behavior [15]. The theory also argues that people engage in humane behaviors for the benefit of society, even if the behaviors sometimes cause them inconvenience. There are three main variables in NAM: Personal Norms (PN), Awareness of Consequences (AC), and Ascription of Responsibility (AR). A personal norm is a "moral obligation to perform or refrain from certain [16]. The term awareness of consequences means, "One is aware of the impact of the consequences of one's behavior on others." Ascription of Responsibility is also described as "one's personal feeling about whether or not s/he is responsible for the negative consequences of not engaging in the desired social behaviors" [17].

Although following the personal norms may increase self-confidence and prevent self-blame, it can also lead to costs, such as extra time and effort. If the benefits of the behavior outweigh its costs to the individual, it is likely that the behavior will be performed. However, if the costs outweigh the benefits, or the costs and benefits are not clear, the person may be hesitant to make a decision. To reduce this skepticism, one may redefine one's understanding of the situation and use defense mechanisms to undermine one's sense of moral commitment. Denying the consequences of not performing such behaviors, which involves underestimating the negative consequences of an action, as well as denying personal responsibility for the behavior, which involves considering it as something beyond control or outside the realm of personal responsibility, are common defense mechanisms in this field [18]. The full implementation of these defense mechanisms neutralizes the individual's moral obligation without imposing punishments on him/her [19]. Two conditions are necessary to overcome such defense mechanisms. First, one must understand that one's behavior affects the well-being of others. Second, the individual must accept personal responsibility for the consequences of his behavior [20]. When these conditions are met, defense mechanisms have less of an impact on his/her performance, and personal norms are more likely to be activated, creating a sense of personal commitment to regulate behavior [21].

2.2. Theory of Planned Behavior (TPB)

The theory of TPB, developed by Azjen [8] is one of the most important and documented frameworks of a socio-psychological theory that tries to logically explain and understand the reason for certain behaviors by individuals [22]. TPB is a generalization of Theory of Reasoned Action (TRA) and has been widely used in the study of ethical behaviors in the information security systems and individual decision-making to adopt acceptable computer security measures and ISSP-compliant behaviors as well as in the field of information security [23].

Azjen [8] stated that a large part of committing a behavior results from a strong decision to do it. The stronger the decision to perform a particular behavior, the more likely a person is to perform that behavior. The TPB theory believes that an individual's decision to engage in behavior is influenced by three psychosocial factors. By carefully considering these three factors, we can predict the likelihood of a particular behavior by the individual. These three factors are a person's attitude toward behavior, perceived behavioral control (PBC), and mental norms.

Attitude is defined as an individual's overall assessment of an object, person, or place, and his or her positive or negative feelings about performing a particular behavior [24]. The more positive a person's attitude toward a behavior, the stronger his or her decision to engage in that behavior. Therefore, attitude can be examined as a fundamental factor in relation to the probability of performing the desired behavior in an individual [25]. However, identifying and extracting a person's attitudes and beliefs is not an easy task. For this reason, there are other variables that affect TPB-related factors. Previous studies have shown that when the behavior in question has an ethical dimension, the individual's norms should be included in the TPB model [26]. Therefore, since ethical dimensions play an important role in conducting behaviors that conform to information security practices, it seems appropriate to pay attention to personal norms in the TPB theory. Mental norms refer to the influence exerted by important people in the individual's life (family, friends, etc.) on his or her behavioral decisions [27]. Getting approval from the important people in a person's life for a behavior has a great impact on motivating him/her to make stronger decisions. Thus, having a high understanding of the associated mental norm can increase the likelihood of a person performing a particular behavior [28]. In addition to examining the reasoned variables that influence a behavior, that is, attitudes toward something and the influence of other people, TPB theory also considers whether a person is fully capable of performing the desired behavior. Each individual has a different capacity to perform planned behaviors, so different default variables may affect his/her planned behavior. PBC is the third component of TPB theory, which defines an individual's perception of the ease or difficulty of performing a particular behavior. Individuals' serious decision to perform a certain behavior is due to the person's high control over himself [29].

In short, the TPB theory predicts that to perform a behavior, people with a more positive attitude toward that behavior, increased approval of others, and more control over the perceived behavior, will make a stronger decision to perform it. The stronger the decision to perform a certain behavior, the more likely a person is to perform that behavior [30].

2.3. Motivation-Opportunity-Ability (MOA) Model

The MOA model was first developed and used to understand consumers' brand information processing methods and their shopping-related behavior [31], which has recently been used extensively in existing studies to explain different types of behavior. In the context of MOA, three main factors influence an individual's behavior, which include "motivation", "necessary skills and abilities" and "opportunities provided" to perform the desired behavior [32]. Motivation examines a person's incentives, concerns, and participation in maintaining information security. Opportunity involves environmental (such as organizational support) and interpersonal (e.g., peer pressure) factors that affect an individual's compliance with information security necessities. Ability examines prior knowledge of information security and skills in interpreting received information [33].

Despite the capacity of the MOA framework for understanding the factors influencing information security compliance behaviors in the workplace, there are many limitations. Admittedly, first, direct measurement of motivation, which is the concern and willingness to comply with information security points, is not possible without taking into account broader dimensions of motivation such as perceived consequences and individual responsibility (NAM theory factors). Second, for the “opportunity” factor, analyzing the effect of peer pressure on individual behavior requires considering a combination of descriptive norms and individual mental norms from TPB theory, which makes it easier to describe interpersonal factors affecting security behaviors. Third, to generalize the concept of ability, it is necessary to examine variables such as actual knowledge (AK) and perceived knowledge of the individual (PK) as well as PBC (from the TPB theory). Therefore, one of the important goals of this study is to integrate the important variables of NAM and TPB theories to strengthen the MOA framework. These proposed variables not only predict information security behaviors, but also inherently complement motivation, opportunity, and ability by definition.

2.4. Conceptual Model and Research Hypotheses

This study is an integrated MOA framework for analyzing the factors affecting behaviors related to human resources information security in the organizational environment, which has been prepared by considering the socio-psychological factors in the model. In the context of MOA, the three main factors, namely motivation, opportunity and ability, are indirect factors affecting behaviors that are not directly observed in this survey but are inferred from other variables. In order to examine the complexity of human behaviors, researchers have recently emphasized the importance of integrating different theories and models for synergistic studies [34]. There is a high potential for using interdisciplinary research approaches, and the knowledge gained in this field can provide new insights into the management of human resource security behaviors in organizations. Many researchers have emphasized that TPB theory is a logical paradigm that ignores the role of irrational and emotional motivations in shaping behavior. In addition, normative activation theory (NAM) is derived only from the heart and states that a person's socializing behavior is due to the activation of his or her personal norms. Accordingly, it seems that TPB and NAM alone may not be sufficient to explain human resource security behaviors [35]. Therefore, in this study, to prepare clear and measurable components for each MOA factor, structures of NAM and TPB theories as well as other variables, identified as indicators of MOA factors in existing models, have been used. It considers the personal and internal goal of the individual to perform the behavior, the external influencing factors and the effects of the external social environment (mental norms) on the individual's behavior. The conceptual model of the present study is shown in Figure 1.

To emphasize the socio-psychological causes affecting the “motivation” factor, the present study considers the three main structures of NAM theory as three indicators of motivation. People usually go through a series of cognitive processes related to their motivation before deciding to start, maintain, or cancel an effort, and all three indices of AC, AR, and PN play an important role in this cognitive dimension of the motivation factor [35, 36]. Attitude - from the TPB theory - is also accepted as the fourth indicator of motivation. Thøgersen [37] also considers attitude as one of the motivational factors in setting behavioral goals. The four dimensions identified are the variables that motivate security behaviors.

The opportunity factor in this study broadly includes all environmental and interpersonal factors that are outside the realm of individual. Therefore, it also includes mental and descriptive norms. In this case, if employees can predict that they can achieve social rewards by accepting social norms, then social norms should be considered as an opportunity [38]. Norms include the social influences that are prevalent in the organizational environment. These social influences can reinforce or inhibit the decision to engage in a behavior, resulting in a situation that is beyond the individual's control. Therefore, norms are considered as constructive variables of the opportunity factor. This study considers three social norms that are consistent with human resource information security practices and affect behaviors. First, subjective norms (SNs), which are a type of emphatic norm in TPB theory and reflect the expectations of others about one's behavior (for example, the majority of co-workers expect employees to turn off their computers when leaving it), include two other important socio-psychological factors, i.e., descriptive norms (DN) and organizational norms (ON). Descriptive norms are observing and understanding the behavior of others in the real world (for example, observing and perceiving whether, in real situations, co-workers behave in accordance with information security practices); Organizational norms also reflect the organization's expectations of the individual's behavior and the degree of commitment or encouragement of the organization to promote the desired behavior (for example, the organization rewards its human resources for observing information security tips). Studies have shown that participation of human resources in community-friendly behaviors is positively associated with organizational support [39]. Positive social norms enhance the perceived opportunity of the individual through social interaction with colleagues. Negative social norms can also limit the individual’s ability to engage in behaviors that conform to information security practices. For example, an employee may not feel comfortable observing information security tips due to selfish coworkers who are unwilling to be bothered to protect customer and organization information. To examine the ability factor, three indicators have been considered, including the individual’s perceived knowledge, the individual’s actual knowledge and PBC from the TPB theory. A person's perceived knowledge refers to his or her personal understanding of his or her knowledge of data protection (for example, updating his or her information about cyber-attacks). In fact, it shows the background knowledge necessary to achieve the desired result. Actual knowledge examines an individual's understanding of information security facts, including that "a website address that starts with http has information security." Perceived knowledge is not always accurate and is also often judged subjectively. Therefore, a standard and correct survey (i.e., actual knowledge) is included in the model. Employees of human resources, like other employees, need training, information systems, coordination, and performance management. Therefore, in order to provide the expected value of business units, the employees of this unit also need training and acquisition of new skills [39, 40]. In addition, PBC complements a person's physical ability with perceived ease to perform a behavior. Based on the research background, we provide hypotheses for MOA framework factors (H1, H2, H3) and for the impact of MOA factors on human resources information security behaviors (H4, H5, H6), which are listed in Table 1. The present study hypothesizes that ability and opportunity are most important if they can be internalized in an individual’s motivation, which shows the mediating effect of motivation on the behaviors suggested in previous studies [41].

Based on the MOA model, the proposed conceptual model consists of three hidden factors of motivation, opportunity and ability as well as 10 variables. This model includes 8 hypotheses that were described earlier. The proposed conceptual model is shown in Figure 1. According to this model, opportunity and ability (each with 3 variables) play the role of independent factors and motivation (with 4 variables) plays the role of mediator, and behavior plays the role of dependent factor.

TABLE 1. Research Hypotheses

	Hypothetical structures of MOA variables
H_1	Motivation factor includes the following indicators: a- Attitude (AT), b- Awareness of consequences (AC), c- Ascription of responsibility (AR) and d- Personal norms (PN).
H_2	Opportunity factor includes the following indicators: a- Subjective norms (SN), B- Descriptive norms (DN) and c- Support for organizational norms (ON).
H_3	The ability factor includes the following indicators: a- Perceived knowledge (PK), B) Actual knowledge (AK) and c) Perceived behavioral control (PBC).
H_4	Motivation factor has a positive and direct effect on information security behaviors.
H_5	Opportunity factor has a positive and direct effect on information security behaviors.
H_6	Ability factor has a positive and direct effect on information security behaviors.
H_7	Opportunity factor has a positive and direct effect on motivation.
H_8	Ability factor has a positive and direct effect on motivation.

3. METHODOLOGY

3.1. Samples and data collection

In this study, a quantitative approach has been used to investigate the impact of MOA factors on behaviors consistent with human resources information security in organizations. The target population of this research is professors and staff from K. N. Toosi University of Technology in Tehran, who deal with students and university information and the Internet more than other staff. One of the reasons for choosing of this university as an statistical population is the lack of integration of university colleges in one place, and attention to human factors can play an effective role in information security of students and university documents.

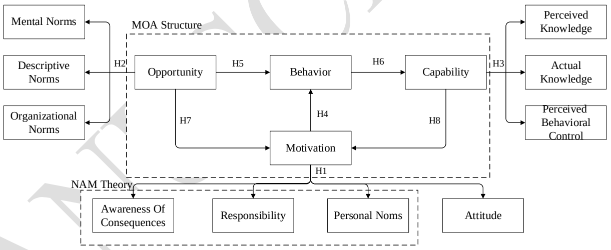

Figure 1. Conceptual model of the study

This survey was conducted in November 2019 by distributing a paper questionnaire among a sample of 200 people, three quarters of whom were professors and staff of various faculties of the university and one third included the staff of the central building of the university. A total of 160 responses were collected. In the process of data pruning, responses with missing values in terms of information security behaviors were deleted. As a result, 141 responses were retained for review.

The final questionnaire consists of 7 items related to demographic characteristics and 33 items related to the conceptual model of the study (motivation, opportunity, ability, security behaviors). Most of these questions have been collected using previous studies related to the subject of research, and some of them have been slightly changed according to the conditions and culture of the community as well as the study environment to be tangible for the respondents. Responses were collected using a 5-point Likert scale with a minimum of 1 and a maximum of 5 and were analyzed by SPSS and LISREL software. Statistics on respondents' demographic characteristics are shown in Table 2.

TABLE 2. Demographic characteristics of the statistical population of the study

Demographic info		**Number**	**(%)**
Gender	Male	70	49
	Female	71	50
Marital status	Single	29	20
	Married	112	80
Education level	Diploma and lower	4	2
	Associate degree	5	3
	Master's degree	44	32
	Masters and above	88	63
Work experience	Under 5 years	14	10
	5-10 years	18	12
	11-15 years	46	33
	16 years and older	63	45
Age	20-30 years	15	11
	31-40 years	62	44
	41-50 years	40	28
	51 years and older	24	17
English language literacy	Beginner	22	16
	Average	79	56
	Advanced	40	28
Level of experience in working with computer/ internet	Beginner	7	5
	Average	78	55
	Advanced	56	40

4. DATA ANALYSIS

The analysis of research hypotheses is performed through second-order structural equation modeling (SEM), in which the structural model describes the relationship between latent variables [42], in which each second-order factor (i.e., motivation, opportunity, and ability) is a combination of several first-order factors (e.g., attitude, awareness of consequences, and personal norms). In this hierarchical structure, first-order factors can be considered as various indicators of second-order ones, and therefore help to understand which specific aspect (i.e., first-order factor) is involved in motivation, opportunity and ability.

According to Table 3, the average of all first-order factors is higher than the median. In addition, the values of skewness and kurtosis of the factors, which are a measure of the normality of the data, are in the range of -0.44 and -0.98.

To fit the measurement model, reliability and validity criteria must be investigated. Reliability of the measurement model is investigated by criteria such as Cronbach's alpha, composite reliability and factor loads. Validity is also two types, convergent validity and diverging validity. Convergent validity is investigated by criteria such as the average variance extracted and divergent and composite reliability with Fornell-Larcker test. The conceptual model fitting algorithm is in Figure 2.

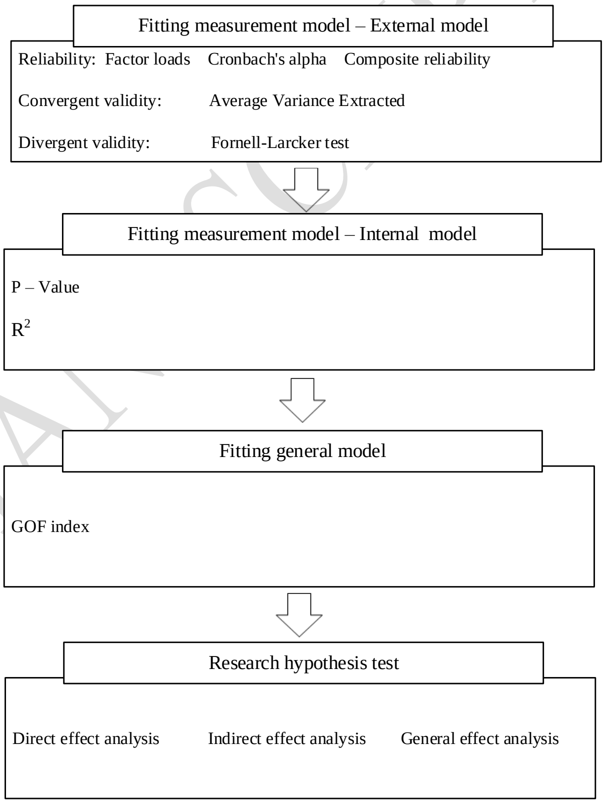
Fitting measurement model – External model
Reliability: Factor loads Cronbach's alpha Composite reliability
Convergent validity: Average Variance Extracted
Divergent validity: Fornell-Larcker test
Fitting measurement model – Internal model
P – Value
R2
Fitting general model
GOF index
Research hypothesis test
Direct effect analysis Indirect effect analysis General effect analysis

Figure 2. Conceptual model fitting algorithm

TABLE 3. Descriptive statistics of first-order factors

First-order factor	**Mean**	**Standard deviation**	**Skewness**	**Kurtosis**
AT	۳/۵۴	۱/۲۲	-۰/۶۹	0.99
AC	۳/۴۸	۱/۱۳	-۰/۶۲	0.97
AR	۳/۵۲	۱/۲۳	-۰/۶۱	0.98
PN	۳/۵۲	۱/۳۰	-۰/۷۱	0.95
DN	۳/۱۹	۰/۸۳	-۰/۵۹	0.96
SN	۳/۱۳	۰/۷۱	-۰/۷۵	-۰/۴۳
ON	۳/۱۰	۰/۷۳	-۰/۵۰	0.96
PK	۳/۴۲	۱/۱۱	-۰/۵۰	0.98
AK	۳/۴۰	۱/۲۰	-۰/۵۴	0.97
PBC	۳/۲۹	۱/۰۴	-۰/۴۴	0.96

According to Table 4, the average of all second-order factors is higher than the median. In addition, the values of skewness and kurtosis of the factors, which are a measure of the normality of the data, are in the range of -43.0 and -0.97. According to Briz-Ponce [10], the normality of data is confirmed in conditions where the values of skewness and kurtosis are in the range of 1 and -1, so, this condition is confirmed for first and second order factors.

TABLE 4. Descriptive statistics of second-order factors

Second-order factor	Mean	Standard deviation	Skewness	Kurtosis
Motivation	۴۲/۱۸	۱۴/۱۹	0.96	-۰/۷۰
Opportunity	۲۸/۲۵	۶/۶۳	0.95	-۰/۶۴
Ability	۳۰/۳۰	۹/۷۰	0.97	-۰/۵۳
Behavior	۱۰/۸۲	۳/۳۳	-۰/۴۶	0.97

4.1 Validity and Reliability

Cronbach's alpha, factor loads and Combined reliability (CR) are the criteria for measuring reliability. Also, the average variance extracted (AVE) and CR were considered as criteria for convergent validity and Fornell-Larcker test for divergent validity. Second-order confirmatory factor analysis was performed to assess: (1) the convergent validity of each first-order factor and (2) whether each of the first-order factors, as assumed in H1, H2, and H3, is a significant portion of its second-order factor (Motivation, opportunity or ability). Factors with a factor load of less than 0.5 were excluded from the hypothetical model [9]. SPSS software was used to calculate Cronbach's alpha, CR and AVE and the Laser software was used to calculate factor loads. The minimum acceptable value for Cronbach's alpha coefficient is 0.7 [25]. The third step in examining convergent reliability is to calculate the Composite reliability. The minimum accepted value for Composite reliability is also considered to be 0.7 [26]. According to Fornell and Larcker [15], the AVE of any structure must be greater than 0.5. The results of convergent reliability and validity calculations are shown in Tables 5 to 9. As the results of convergent reliability and validity calculations show that the factor load of all items is more than 0.5 and Cronbach's alpha coefficient of all factors is higher than 0.7. Therefore, the reliability of the present study is supported. In the convergent validity test, for all first-order factors, AVE is higher than the suggested threshold (from 0.61 to 0.88) and CR is satisfactory (from 0.80 to 0.98), and AVE and CR are also acceptable for second-order factors (Table 9), which supports the convergent validity of the study. Divergent validity is also supported because the value of the AVE root of the latent variables in the major diameter of the matrix is greater than the value of the correlation between them in the lower and left cells of major diameter (according to Table 10). According to these results, it can be said that convergent reliability and validity have been confirmed.

Table 5 statistics of fit of hidden variable and survey items related to motivation factor, Table 6 statistics of fit of hidden variable and survey items related to opportunity factor, Table 7 statistics of fit of hidden variable and survey items related to ability factor, are available in appendix section.

Table 8. Statistics of fit of hidden variable and survey items related to behavior factor

Hidden variables	Item	standard deviation SD	Factor load	AVE	Combined relibility	Cronbach's alpha
Information security behaviors	Because forgetting multiple passwords is probable, I use the same password for all my accounts.	۱/۰۱	۰/۹۲	0.86	0.98	0.95
	When someone sends me a link, I open it without making sure the link is valid.	۱/۲۸	۰/۹۳			
	I will create a backup of my important information.	۱/۱۹	۰/۹۴			

As shown in the results of convergent reliability and validity calculations, according to Table 9, the factor load of all second-order factors are greater than 0.5 and the Cronbach's alpha coefficient of all factors is higher than 0.7. Therefore, the reliability of the present study is supported. For the second-order factors, AVE and CR are also acceptable in the convergent validity test, which supports the convergent validity of the study.

TABLE 9. Statistics of fit of second-order factors

Second-order factor	First-order factor	Factor load	AVE	Combined reliability	Cronbach's alpha
	AT	0.98			
Motivation	AC	0.94	0.92	0.99	0.98
	AR	0.95			
	PN	0.97			
	DN	0.97			
Opportunity	SN	0.92	0.89	0.98	0.96
	ON	0.96			
	PK	0.95			
Ability	AK	0.97	0.90	0.99	0.96
	PBC	0.91			

To calculate the Fornell-Larcker index, the value of the AVE root of the latent variables in the major diameter of the matrix must be greater than the correlation between those arranged in the lower and left cells of the original diameter [14]. In this study, the value of the AVE root of the hidden variables in the major diameter of the matrix is greater than the correlation value between them in the lower and left cells of the major diameter (Table 8).

TABLE 10. Divergent validity by Fornell-Larcker test

Factor	AT	AC	AR	PN	DN	SN	ON	PK	AK	PBC
AT	۰/۹۰									
AC	۰/۸۸	۰/۹۱								
AR	۰/۸۸	۰/۹۰	۰/۹۳							
PN	۰/۸۹	۰/۸۹	۰/۹۱	۰/۹۲						
DN	۰/۸۸	۰/۸۵	۰/۸۶	۰/۸۷	۰/۸۹					
SN	۰/۸۵	۰/۸۳	۰/۸۴	۰/۸۵	۰/۸۷	۰/۷۸				
ON	۰/۸۷	۰/۸۵	۰/۸۵	۰/۸۵	۰/۸۸	۰/۷۷	۰/۸۰			
PK	۰/۸۷	۰/۸۷	۰/۸۸	۰/۸۵	۰/۸۷	۰/۷۵	۰/۷۷	۰/۹۱		
AK	۰/۸۸	۰/۸۶	۰/۸۹	۰/۸۷	۰/۸۸	۰/۷۶	۰/۷۹	۰/۹۰	۰/۹۴	
PBC	۰/۸۱	۰/۸۳	۰/۸۲	۰/۸۱	۰/۸۶	۰/۷۳	۰/۷۵	۰/۸۸	۰/۸۸	۰/۹۰

4.2 Structural model analysis

The internal model describes the relationship between the hidden variables. To evaluate the internal model, the path coefficient, t-statistic and coefficient R^2 (variance of each factor) must be calculated. In the present study, all the criteria required for structural model analysis have been calculated by SPSS software. Path coefficients represent the overlap level between the two hidden variables. In other words, the path coefficient indicates the existence of a linear causal relationship and the intensity and direction of this relationship between the two hidden variables. The path correlation coefficient is a number between +1 and -1. A value of zero means that there is no linear relationship between the two hidden variables. According to Table 11, the magnitude of the significance coefficients t for all relations in the model is greater than 1.96, which means that the path coefficient is accepted at the significance level of 95%. Also, since the value of p statistic for all available relations is less than 0.05, all hypotheses are confirmed.

TABLE 11. Hypotheses of the internal model

Number	Hypotheses	Path correlation	T statistic	P value	Confirmed?
1	Motivation→ Behavior	0.040	32.597	0.000	yes
2	Opportunity→ Behavior	0.061	52.330	0.000	yes
3	Ability→ Behavior	0.846	34.648	0.000	yes
4	Opportunity→ Motivation	0.446	19.23	0.000	yes
5	Ability→ Motivation	0.495	21.29	0.000	yes

The coefficient R^2 is a criterion used to correlate the measurements and the structural equation modeling and shows the effect of an independent variable on a dependent variable. The higher the coefficient of determination related to the dependent variables of a model, the better the model fits. Three values of 0.25, 0.5 and 0.75 are considered as the criterion values for weak, medium and strong values of R^2 [14, 15].

TABLE 12: Coefficients of determination of dependent variables

Dependent variable	Coefficient of determination (R^2)
Behavior	0.883
Motivation	0.858

5. DISCUSSION

In this study, which was based on the MOA model, the results confirm that awareness of consequences, ascription of responsibility, personal norms and attitudes play a role in creating the motivating factor. Subjective norms, descriptive norms, and organizational norms help create the opportunity factor. Perceived behavioral control, perceived knowledge, and actual knowledge play a role in creating the ability factor. It can also be concluded that ability, opportunity and motivation directly affect the information security behaviors of organizational human resources, where, the effect of ability is more than opportunity and that of opportunity more than motivation. Also, the two factors of opportunity and ability affect the behavior of organizational human resources indirectly and through the motivation mediatory factor. According to the results, the mediating effect of motivation in the relationship between the ability and behavior is less than 8%, which is ignorable. According to the VAF concept proposed by Zhao et al. [41], it can be inferred:

- Considering the coefficient of 0.079 as the total effect of the opportunity factor on the behavior factor, 23% of the total effect is indirect,

going through the following path: opportunity → motivation → behavior (0.079 ÷ 0.040 × 0.446).

- 77% of the total effect of opportunity factor on behavior is a direct effect, going through the path: opportunity → behavior (0.079 ÷ 0.061).
- Considering the coefficient of 0.866 as the total effect of the ability factor on the behavior factor, 3% of the total effect is indirect, going through the following path: ability → motivation → behavior (0.866 ÷ 0.040 × 0.495).
- 97% of the total effect of ability factor on behavior is a direct, going through the following path: ability → behavior (0.866 ÷ 0.846).

Considering these values and the prominent effect of “ability” in human resource security behaviors, it can be concluded that holding the necessary training courses to enhance information level and employees' abilities for information security can motivate people to maintain security and also improve their security behaviors. In addition, creating organizational norms in the form of financial and social rewards for observing information security tips in the organization as well as creating a demanding culture among employees (for example, if your colleague does not pay attention to information security tips, ask him to reconsider his behavior), can be useful strategies to improve perceived employee opportunities, which in turn improves security motivation and behaviors. Organizational efforts can also focus on exerting beneficial normative influence in the organization to increase social norms. Conducting personality tests on employees can also help managers (especially human resources managers) to plan and implement appropriate strategies correspondent to personal differences in order to know the employees' subjective norms, personal norms and to some extent, their attitude and responsibility in order to maintain the security of the organization's information as much as possible.

5.1. Research Limitations and Recommendations for Future Research

In carrying out any research project, obstacles and limitations emerge on the way. This study is no exception and therefore, we indicate the existing barriers and limitations. One of these limitations is the measurement tool used in this study, because in this study, a questionnaire was used to collect data, the inherent limitations of the questionnaire, such as superficial consideration of real events and scalability can prevent attaining real results and the respondents have encountered perceptual errors in answering the questions. Accordingly, new methods can be used for data collection in future research. Also, in this study, a total of 141 questionnaires have been analyzed for data collection. Naturally, increasing the number of questionnaires and consequently increasing the number of available data can increase the consistency and validity of the results. It should also not be overlooked that the moderator variable was not used in this study. In general, the use of adjusting variables such as gender, age, work experience, etc. could provide more comprehensive and accurate results. With the variables defined in each of the MOA factors, this framework can be used as a diagnostic tool to identify the limiting factors of information security behaviors in a particular organization and can become the basis for future studies to identify the right strategies in order to maintain information security and thus help decision makers to create more efficient and targeted executive programs to promote behavior change.

6. REFERENCES

1. Hoffmann R., Napiórkowski J., Protasowicki T. , Jerzy Stanik, "Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach", 1st International Conference on Optimization-Driven Architectural Design, (2020), https://doi.org/10.1016/j.promfg.2020.02.244.

2. Zare M. R., Aghaie A., Samimi Y., A. Hadad Asl, "A Novel Excellence Model of the Information and Communications Technology Industry: Case Study on Telecommunications Backbone Network of Iran", ***International Journal of Engineering, Transactions A: Basics, Vol. 33, No. 10***, (2020) 2016-2029, https://doi: 10.5829/ije.2020.33.10a.20.

3. Roberts D. J., An Analysis of employee information security policy compliance behaviour: A generic qualitative inquiry, Capella University, 2021.

4. Jeyanthi N., Shabeeb H., M. Saleem A. Durai, Thandeeswaran R., "Reputation Based Service for Cloud User Environment", ***International Journal of Engineering, Transactions B: Applications***, Vol. 27, No. 8 (2014) 1179-1184, https:// doi: 10.5829/idosi.ije.2014.27.08b.03.

5. Kwesi Hughes-Lartey, Meng Li, Francis E. Botchey, Zhen, "Human factor, a critical weak point in the information security of an organization's Internet of things", Heliyon,(2021), , https://doi.org/10.1016/j.heliyon.2021.e06522.

6. Karjalainen M., Siponen M., Sarker S., "Toward a stage theory of the development of employees' information security behaviour", ***Computers & Security***, (2020) https://doi.org/10.1016/j.cose.2020.101782.

7. Bagheri Z., Safaie N., Strategic planning of human resources based on BSC model, ***Quarterly Journal of Human Resource Management Research***, Imam Hossein University, 8th year, consecutive issue 25 (Fall 2016), p: 159 -181. (2016).

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

9. Bagozzi, R. P., & Yi, Y. Specification, evaluation, and interpretation of structural equation models**.** ***Journal of the Academy of Marketing Science***, Vol. 40(1), 8-34, (2012),https://doi.org/10.1007/s11747-011-0278-x.

10. Briz-Ponce, L., Pereira, A., Carvalho, L., Juanes-Méndez, J. A., & García-Peñalvo, F. J. Learning with mobile technologies–Students' behavior. ***Computers in Human Behavior***, 72, 612-620, (2017). https://doi.org/10.1016/j.chb.2016.05.027.

11. Carlton M., Levy Y., "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals." *SoutheastCon 2015*, IEEE. (2015), https://doi.org/ 10.1109/SECON.2015.7132932.

12. Evans, M. "Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector." ***International journal of medical informatics*** 127 109-119, (2019), https://doi.org/10.1016/j.ijmedinf.2019.04.019.

13. Hamidi, H., Vafaei, A. and Monadjemi, S.A. (2012). Analysis and Evaluation of a New Algorithm Based Fault Tolerance for Computing Systems. International Journal of Grid and High Performance Computing (IJGHPC), 4(1), 37-51. doi:10.4018/jghpc.2012010103

14. Schwartz, Shalom H., "Normative influences on altruism." *Advances in* experimental social psychology. Vol. 10. Academic Press, 221-279, (1977), https://doi.org/10.1016/S0065-2601(08)60358-5.

15. Fornell, C., & Larcker, D. F. Evaluating structural equation models with unobservable variables and measurement error. ***Journal of Marketing Research***, 18(1), 39-50, (1981), https://doi.org/10.1177/002224378101800104.

16. Gao, L., "Application of the extended theory of planned behavior to understand individual's energy saving behavior in workplaces***." Resources, Conservation and Recycling*** 127, 107-113, (2017) https://doi.org/10.1016/j.resconrec.2017.08.030.

17. Gandel, Lloyd's CEO: Cyber-attacks cost companies 400 billion every year,(2015). http://fortune.com/2015/01/23/cyber-attack-insurancelloyds/(accessed 03 October 2018).

18. Gratian, M., Bandi S., Cukier M., Dykstra J., Ginther A.,"Correlating human traits and cyber security behavior intentions." ***Computers & Security*** 73, 345-358, (2018) https://doi.org/10.1016/j.cose.2017.11.015.

19. Hair, J. F., Ringle, C. M., & Sarstedt, MPLS-SEM, " Indeed a silver bullet". ***Journal of Marketing theory and Practic****e*,19(2),139-152,(2011). https://doi.org/10.2753/MTP1069-6679190202.

20. Altabash K., Happaa b., "Insider-threat detection using gaussian mixture models and sensitivity profiles." ***Computers & Security*** 77,838-859., (2018) https://doi.org/10.1016/j.cose.2018.03.006.

21. Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory." ***Computers &Security*** 31.1,83-95, (2012),https://doi.org/10.1016/j.cose.2011.10.0076.

22. Kuru, Damla, and Sema Bayraktar, "The effect of cyber-risk insurance to social welfare." ***Journal of Financial Crime*** 24.2 ,329-346, (2017), https://doi.org/10.1108/JFC-05-2016-0035.

23. Xu, X., Chen C., Menassa C., "Understanding energy-saving behaviors in the American workplace: A unified theory of motivation, opportunity, and ability." ***Energy Research & Social Science*** 51, 198-209, (2019), https://doi.org/10.1016/j.erss.2019.01.020.

24. Malekinezhad, F., Bin H. L. Investigation into University Students Restoration Experience: The Effects of Perceived Sensory Dimension and Perceived Restrictiveness, (2017), https://doi.org/doi: 10.20944/preprints201708.0085.

25. Michie S., Stralen, M., West, R., "The behaviour change wheel: a new method for characterising and designing behaviour change interventions." ***Implementation science*** 6.1, 42, (2011), https://doi.org/10.1186/1748-5908-6-42.

26. Nummally, J., Psychometric Theory. McGraw-Hill, Retrieved from. 1978. https://books.google.com/books/about/Psychometric_theory.html?id= WE59AAAAMAAJ>.<

27. Osterhus, Thomas L., "Pro-social consumer influence strategies: when and how do they work? " ***Journal of Marketing*** 61.4,16-29,(1997), https://doi.org/10.1177/002224299706100402.

28. Hamidi, H ,Vafaei, A., and Monadjemi, A. H., "Algorithm Based Fault Tolerant and Check Pointing for High Performance Computing Systems", ***Journal of Applied Sciences***, vol. 9, no. 22, pp. 3947–3956, 2009. doi:10.3923/jas.2009.3947.3956.

29. Hamidi, H., & Mohammadi, K. (2006). Modeling Fault Tolerant and Secure Mobile Agent Execution in Distributed Systems. International Journal of Intelligent Information Technologies (IJIIT), 2(1), 21-36. doi:10.4018/jiit.2006010102

30. Rezaei, R.., "Drivers of farmers' intention to use integrated pest management: Integrating theory of planned behavior and norm activation model." ***Journal of Environmental Management*** 236,328-339,(2019) https://doi.org/10.1016/j.jenvman.2019.01.097.

31. Sohrabi Safaab N., Maplea C., Watson T., Von Solms B., (2018), "Motivation and opportunity-based model to reduce information security insider threats in organisations." ***Journal of Information Security and Applications*** 40,247-257,(2018), https://doi.org/10.1016/j.jisa.2017.11.001.

32. Schwartz, Shalom H., "Normative explanations of helping behavior: A critique, proposal, and empirical test." ***Journal of Experimental Social Psychology*** 9.4, 349-364,(1973), https://doi.org/10.1016/0022-1031(73)90071-1.

33. Schmidt, K., "Predicting the consumption of expired food by an extended Theory of Planned Behavior***." Food Quality and Preference*** 78, 103746,(2019), https://doi.org/10.1016/j.foodqual.2019.103746.

34. Shan, J., Jingmei, L., and Zhihua, X., "Estimating ecological damage caused by green tides in the Yellow Sea: A choice experiment approach incorporating extended theory of planned behavior***." Ocean & Coastal Management*** 181,104901,(2019), https://doi.org/10.1016/j.ocecoaman.2019.104901.

35. Hamidi, H., Vafaei, A. and Monadjemi, S.A., Analysis and design of an ABFT and parity-checking technique in high performance computing SYSTEMS. Volume., 21, No. 3. Journal of Circuits, Systems and Computers, Vol. 21, No. 03, 1250017 (2012) , https://doi.org/10.1142/S021812661250017X

36. Sohrabi Safa N., Solms R., Futcher, L.," Human aspects of information security in organisations"***. Computer Fraud & Security***.2,15-8,(2016), https://doi.org/10.1016/S1361-3723(16)30017-3.

37. ThØgersen, J., "Understanding of consumer behaviour as a prerequisite for environmental protection." ***Journal of Consumer Policy Vol.*** 18, No. 4, 345-385,(1995), https://doi.org/10.1007/BF01024160.

38. Wilson, C., and Melissa R. , "Insights from psychology about the design and implementation of energy interventions using the Behaviour Change Wheel." ***Energy Research & Social Science*** 19,177-191,(2016), https://doi.org/10.1016/j.erss.2016.06.015.

39. Wolske, K. S., Paul, C., and Thomas, D., "Explaining interest in adopting residential solar photovoltaic systems in the United States: Toward an integration of behavioral theories***." Energy Research & Social Science*** 25, 134-151,(2017).

40. Yazdanmehr, A., and Jingguo W. "Employees' information security policy compliance: A norm activation perspective." ***Decision Support Systems*** 92 , 36-46,(2016), https://doi.org/10.1016/j.erss.2016.12.023.

41. Zhao, X., Lynch Jr, J. G., & Chen, Q., “Reconsidering Baron and Kenny: Myths and truths about mediation analysis”. ***Journal of Consumer Research***, 37(2), 197-206, (2010) https://doi.org/10.1086/651257.

42. Torabi, A., Hamidi, H., Safaie, N., “Effect of Sensory Experience on Customer Word-of-mouth Intention, Considering the Roles of Customer Emotions, Satisfaction, and Loyalty”, ***International Journal of Engineering, Transactions C: Aspects, Vol. 34, No. 3***, (2021) 682-699, https://doi.org/10.5829/ije.2021.34.03c.13.

7. Appendix

Table 5. Statistics of fit of hidden variable and survey items related to motivation factor

Hidden variables	Item	standard deviation SD	Factor load	AVE	Combined reliability	Cronbach's alpha
	Adherence to workplace information security tips is essential.	۱/۲۰	۰/۹۰			
Attitude (AT)	Holding information security training courses for the organization's employees is a waste of time and money.	۱/۳۵	۰/۹۲	۰/۸۲	۰/۹۶	۰/۹۳
	Accomplishing a project in less time and with lower information security levels is better than accomplishment of the project in more time but with higher information security.	۱/۳۴	۰/۹۰			
	Observance of workplace information security tips will have positive consequences for the organization.	۱/۱۶	۰/۹۲			
Awareness of Consequences (AC)	By observing the information security of the workplace, I will play a beneficial role for my organization.	۱/۲۰	۰/۹۱	۰/۸۳	۰/۹۶	۰/۹۳
	Non-observance of workplace information security tips will have adverse consequences for the organization's customers.	۱/۲۴	۰/۹۰			
	Because my involvement in information security is ignored by the organization, I do not feel responsible for complying with my workplace security tips.	۱/۳۸	۰/۹۵			
Ascription of Responsibility (AR)	The responsibility for information security of my workplace lies with the organization itself, not me.	۱/۳۲	۰/۹۴	۰/۸۶	۰/۹۷	۰/۹۵
	I feel responsible for adhering to workplace information security tips.	۱/۱۶	۰/۸۹			
	I feel guilty when I do not follow the information security tips in performing my duties.	۱/۳۴	۰/۹۱			
Personal norms (PN)	No matter how others behave, I feel morally obligated to follow the information security tips of my workplace.	۱/۴۱	۰/۹۴	۰/۸۵	۰/۹۷	۰/۹۵
	I feel good when I follow the information security tips.	۱/۳۵	۰/۹۲			

Table 6. Statistics of fit of hidden variable and survey items related to opportunity factor

Hidden variables	Item	standard deviation SD	Factor load	AVE	Combined reliability	Cronbach's alpha
	My colleagues are concerned about workplace security vulnerabilities.	۰/۹۲	۰/۹۳			
Descriptive norms (DN)	My colleagues pay attention to information security in the performance of their duties.	۰/۹۴	۰/۹۴	0.80	0.94	0.92
	My colleagues work to ensure the safety of workplace information.	۰/۸۴	۰/۷۹			
	My colleagues expect me to lock or shut down my system when it leaves.	۰/۸۲	۰/۷۸			
Subjective norms (SN)	My colleagues expect me to be aware of the presence of strangers when giving confidential information.	۰/۸۳	۰/۷۹	0.61	0.80	0.82
	My colleagues expect me not to connect my personal communication devices such as cell phones, flash memories, etc. to workplace systems.	۰/۸۳	۰/۷۸			

Organizational norms (ON)	My organization rewards its employees (in various ways) for adhering to information security tips.	۰/۸۴	۰/۷۸	0.64	0.84	0.85
	Observing information security tips in my workplace is defined as an organizational culture and value.	۰/۸۳	۰/۸۱			
	The leadership and management of my organization strive to provide in-house training courses to increase employee awareness of information security.	۰/۸۵	۰/۸۲			

Table 7. Statistics of fit of hidden variable and survey items related to ability factor

Hidden variables	Item	standard deviation SD	Factor load	AVE	Combined reliability	Cronbach's alpha
Perceived Knowledge (PK)	I'm constantly updating my knowledge of cyberattack malware and data theft methods.	۱/۰۲	۰/۹۰	۰/۸۳	۰/۹۶	۰/۹۳
	I know how to use the firewall and update my system security software.	۱/۱۸	۰/۸۹			
	I how to make the deleted files irrecoverable.	۱/۳۲	۰/۹۵			
Actual Knowledge (AK)	The website address that starts with http guarantees information security.	۱/۴۳	۰/۹۲	۰/۸۸	۰/۹۸	۰/۹۴
	I am familiar with more than three of the following concepts. -Phishing attacks -Social engineering attacks -DDOS attacks -Cloud database -Multi-factor authentication	۰/۹۷	۰/۹۹			
	Before downloading a file, it can be checked to see if it's a virus.	۱/۳۴	۰/۹۱			
Perceived Behavioral Control (PBC)	I'm sure I can follow my workplace information security tips if I want to.	۰/۹۸	۰/۸۵	۰/۸۱	۰۹۴	۰/۹۲
	It's entirely up to me whether I follow my job security tips.	۱/۰۹	۰/۸۷			
	Applying information security methods in my workplace is completely under my control.	1.27	۰/۹۷			

Persian Abstract

چکیده

امنیت اطلاعات یک مسأله حیاتی است که امروزه سازمان ها در سراسر دنیا با آن روبرو هستند. در حال حاضر سیل عظیمی از حملات سایبری و تهدیدات امنیتی ناشی از سهل انگاری عوامل انسانی اتفاق می افتد که این امراهمیت رفتار منابع انسانی در سازمان را دوچندان می‌کند. پژوهش حاضرچارچوبی یکپارچه از انگیزه فرصت-توانایی (MOA) را ارائه می دهد که شامل عوامل روانشناختی اجتماعی از مدل NAM و نظریه TPB برای بررسی متغیرهای تعیین کننده رفتارهای امنیتی در یکی از دانشگاه های معتبر تهران است. برای این منظور اطلاعات با توزیع ١٤١ پرسشنامه بین کارکنان این دانشگاه، جمع آوری شده و مورد تحلیل قرار گرفته است. فرضیه های تحقیق، از روش مدل سازی معادلات ساختاری (SEM) و با استفاده از نرم افزار SPSS و Lisrel مورد بررسی و آزمون قرار گرفته است. نتایج حاصله نشان می دهد که توانایی بیشترین تأثیر را در رفتارهای امنیت اطلاعات دارد و به دنبال آن فرصت و انگیزه، به ترتیب تأثیر مستقیم و معناداری بر رفتار دارند. علاوه بر این، انگیزه، میانجی گر تأثیر فرصت و توانایی است. در انتها پیشنهادهایی برای طراحان استراتژی های مؤثر امنیت اطلاعات بر اساس عوامل محدود کننده رفتار منابع انسانی در سازمان ارایه گردیده است.

کلیدواژه ها: امنیت اطلاعات؛ رفتار منابع انسانی؛ مدل MOA؛ تئوری NAM؛ تئوری TPB