Factors affecting information security protection behaviors with the mediation of fear and motivation to protect information

Eisa Bigdeli
Islamic Azad University, Iran
eisa.bigdeli67@gmail.com

Fariba Nazari
Azad University, Iran
fnazari@iau.ac.ir

Abstract. *This research was conducted with the aim of investigating the factors influencing information security protection behaviors with the mediating role of fear and motivation to protect information based on the theories of protection motivation and planned behavior among the employees of the telecommunications company in Khuzestan region of Iran. This study is of an applied-survey type. The statistical population included the employees of Khuzestan telecommunications company, who were selected using Cochran's formula of 311 by non-random sampling method. The data collection tool was designed based on a questionnaire. In data analysis, structural equation modeling was used to fit the model and test research hypotheses using SPSS, SmartPLS software. The results showed organizational commitment, job satisfaction, fear, self-efficacy, attitude, and mental norms has a significant effect on the motivation to protect information. In addition, sensitivity to threat, and intensity of threat had a significant effect on fear. Information protection motivation had a positive effect on information security protection behaviors. However, the cost of responding and perceived behavioral control did not affect the motivation to protect information.*

Keywords: *Information security protective behaviors; fear; information protection motivation; protection motivation theory; theory of planned behavior.*

Factores que influyen en los comportamientos de protección de la seguridad de la información: el papel mediador del miedo y la motivación para proteger la información

Resumen. *El objetivo de esta investigación es analizar los factores que influyen en los comportamientos de protección de la seguridad de la información, considerando el papel mediador del miedo y de la motivación para proteger la información. El estudio se basa en la teoría de la motivación para la protección y en la teoría del comportamiento planificado, y se desarrolla en el contexto de los empleados de la empresa de telecomunicaciones de la región de Juzestán, en Irán. Se trata de un estudio de tipo aplicado y de carácter empírico. La población estadística estuvo compuesta por los empleados de la empresa de telecomunicaciones de Juzestán, de los cuales se seleccionó una muestra de 311 participantes mediante la fórmula de Cochran, utilizando un método de muestreo no aleatorio. La recogida de datos se llevó a cabo mediante un cuestionario. Para el análisis de los datos, se empleó el modelado de ecuaciones estructurales con el fin de ajustar el modelo y contrastar las hipótesis de investigación, utilizando los programas SPSS y SmartPLS. Los resultados muestran que el compromiso organizacional, la satisfacción laboral, el miedo, la autoeficacia, la actitud y las normas subjetivas tienen un efecto significativo sobre la motivación para proteger la información. Asimismo, la sensibilidad a la amenaza y la severidad de la amenaza influyen de manera significativa en el miedo. La motivación para proteger la información presenta un efecto positivo sobre los comportamientos de protección de la seguridad de la información. Sin embargo, el coste de la respuesta y el control conductual percibido no mostraron un efecto significativo sobre la motivación para proteger la información.*

Palabras clave: *comportamientos de protección de la seguridad de la información, miedo, motivación para la protección de la información, teoría de la motivación para la protección, teoría del comportamiento planificado.*

1. Introduction

The impressive global growth and development of information and communication technologies in recent years has led to new and numerous applications of its technologies and services, and as a result of this increased use, the amount of use of these technologies has also increased. Although the growth of the use of information technology and information systems can be seen as a result of their convenience, organizations in relation to them are facing a problem called data theft and data breach (Giao et al., 2020). The rapid development of information-based technologies and services has led to a great reliance on information security to protect organizational data (Zhang et al., 2017). Security refers not only to encryption, secure communications, and privacy assurance, but also to employee protective behaviors. Information security relies on a highly efficient authentication and authorization system to access corporate databases that hold valuable personal and business-sensitive information. Therefore, it is also affected by internal information violations in organizations (Safa & Ismail, 2013). Employees should ensure that they consider potential privacy vulnerabilities, security holes, etc. to provide system protection (Li et al., 2016). Therefore, employees are at the forefront of the concept of security (Jang-Jaccard & Nepal, 2014; Posey et al., 2015).

Safa et al. (2015) reported that the main reason for information security flaws is the fact that employees are the most vulnerable link in the security chain. On the one hand, their activity is necessary for the survival of the organization, and on the other hand, they are a significant threat to the organization. For example, between March and October 2016, an IT expert at a well-known Internet company in China sold more than 155,000 items of personal information, including home addresses, work units, and salaries, to a Beijing-based technology company. This action led to severe consequences for the company, including financial loss, reputational damage, and allegations of privacy violations. Hence, attention and focus on the emergence of information security protective behaviors (Crossler et al., 2013) as the behaviors of organizational members that affect the availability, relevance, confidentiality, and integrity of information security. They say it is a useful approach for organizations (Sommestad et al., 2019).

Protection motivation theory is a behavioral science theory that was originally developed to predict and explain behaviors influenced by a person's threat appraisal (which is an exciting and intense negative outcome) and coping appraisal (the degree to which people's behavior is effective in eliminating danger). Also, researchers in the field of information security also consider the theory of planned behavior, which is a well-established behavioral scientific

theory, useful for determining the predictors of information security behaviors (Ajzen, 2002). The theory of planned behavior believes that behavior is determined by a set of beliefs that can be grouped into attitudes, mental norms, and perceived behavioral control (Sommestad et al., 2019). This study combines both theories to provide a more complete representation of the ways in which perceptual and attitudinal factors influence behavior. On the other hand, previous studies have tried to use research frameworks that integrate the theories of protection motivation and planned behavior with other constructs (Bulgurcu et al., 2010; Herath & Rao, 2009; Lee & Larsen, 2009) but few work-related factors that deeply affect employee performance in an organizational setting have been considered. Since researchers have shown that both individual and organizational factors are worth discussing, behavioral researchers should not ignore the impact of job satisfaction and organizational commitment on security performance and willingness to protect information security resources (Chang et al., 2012; Ma, 2022).

Moreover, the conducted studies have shown that the certainty of official sanctions against deviant behaviors of information security, as a tool for official social control, cannot fully explain the protection of information security. This is consistent with previous studies that examined information security breaches from a rational choice perspective (Cheng et al., 2013; Vance & Siponen, 2012).

To address this research gap and strengthen the field's understanding of employees' information security protective behaviors, this study focuses on insights from behavioral and attitudinal perspectives. In recent years, vulnerabilities in modern technologies, distributed systems, network integration, performance of data processing systems and applications, and telecommunication networks have caused so that issues related to information security and information protection become very important for Khuzestan province telecommunications company. The present study aims to investigate information security protection behaviors among the employees of Khuzestan Telecommunication Company by combining two protection motivation theories (threat sensitivity, threat severity, self-efficacy and response cost) and planned behavior (attitude, perceived behavioral control and subjective norms) and job-related organizational factors (organizational commitment and job satisfaction) and tries to answer the fact that the effective factors on information security protection behaviors with the mediating role of fear and motivation to protect information based on the theory: What are the motivations of protection and planned behavior among the employees of Khuzestan telecommunication company in Iran?

2. Literature review

The growing threat of cyberattacks has elevated information security (IS) as a critical pillar for organizational survival, with information now serving as a company's core capital (Kim & Choi, 2002). Effective IS practices safeguard sensitive data, enabling compliance with best practices and mitigating risks (Plachkinova & Maurer, 2018). This study explores factors influencing IS protection behaviors among telecommunication employees, emphasizing fear and motivation as mediators, grounded in protection motivation theory (PMT) and the theory of planned behavior (TPB).

While PMT has been a prominent framework in understanding information security compliance, previous research has produced inconsistent findings regarding its factors' effects on compliance behavior, necessitating further empirical validation. Moreover, the majority of research has been carried out in developed countries. The data were collected from 210 bank employees in Yemen and analyzed using PLS-SEM. This research showed that perceived self-efficacy, response efficacy, and severity significantly influence the employees' intentional behavior in complying with information security policies. However, the results did not support the hypotheses of perceived response cost and perceived vulnerability. This study also discussed both theoretical and practical implications of enhancing information security compliance behavior (Alrawhani et al., 2025). This study aimed to examine the complex interplay between perceived threat severity, perceived threat vulnerability, fear, perceived response efficacy, perceived self-efficacy, and response cost grounded in the PMT. The analysis was situated within the context of cybersecurity and information security in Industry Revolution 4.0 (IR 4.0) environments, where interconnected systems are increasingly exposed to cyber threats. Findings demonstrate that perceived threat severity and vulnerability significantly increased fear, which mediated the threat perception-protection motivation relationship, emphasizing the role of emotional responses in indecision-making. Coping appraisal components, namely perceived response efficacy and self-efficacy, were strong positive predictors of protection motivation, while response cost negatively influenced protective behavior intentions. Although intrusion detection systems are essential in mitigating cyber risks, this study highlighted the equally critical behavioral component of cyber defense (Abd Latif et al., 2025).

Research underscores the role of organizational policies, employee attitudes, and theoretical frameworks in shaping IS compliance. Safa & von Solms (2016) found that security knowledge-sharing, cooperation, and personal norms

influence attitudes toward IS policies, though affiliation does not affect compliance intentions. Alshare et al. (2018) highlighted that employee involvement in IS policy design can reduce violations, while consistent sanction enforcement deters breaches. Tang et al. (2021) demonstrated that government social media engagement during crises boosts IS behaviors via perceived severity, self-efficacy, and response effectiveness. Ma (2022) linked IS attitudes, subjective norms (TPB), and coping/threat appraisals (PMT) to protection behaviors, though job satisfaction and perceived behavioral control showed no significant impact. Despite these advancements, empirical research on IS protection behaviors remains limited, particularly in domestic contexts. This study addresses this gap by examining job-related organizational factors, PMT, and TPB among Khuzestan Telecommunications Company employees. It emphasizes the need to analyze employee attitudes and behaviors to mitigate IS risks, aligning with calls for localized research to strengthen organizational security frameworks.

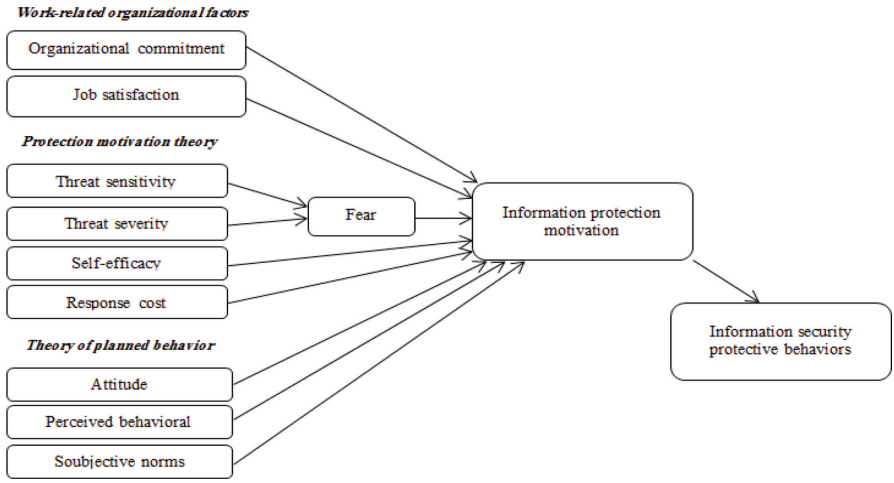
This research can provide solutions to reduce security problems. Thirdly, information security protection behaviors have a short life and history, and for this reason, it is considered a virgin and attractive topic for researchers. Today, Khuzestan region telecommunication company is looking for information security, and in this regard, paying attention to the behaviors and desires of employees in the field of protecting information security is a big step in the direction of improving information security. Considering the importance of information security protection behaviors among the employees of Khuzestan Telecommunications Company, the results of this research can help to prevent waste of resources and improve productivity for the company, individuals and society. Figure 1 shows a view of the conceptual model of the research.

According to Figure 1, twelve subscales in six components include organizational commitment, job satisfaction, threat sensitivity, threat severity, self-efficacy, response cost, attitude, perceived behavioral control, and subjective norms as independent variables and fear variables and protection motivation. Information as mediating variables and information security protective behaviors as dependent variables are the criterion or final, and these components and subscales are defined as follows.

2.1 Behaviors protecting information security and its importance

Increasing data and network security is becoming one of the most urgent tasks in organizational, corporate and private communications. The exchange of information is very vital and sensitive, which should be considered

Figure 1. Research model (Ma, 2022)



sufficiently through the Internet and networks by employees through the occurrence of protective behaviors (Mojisola et al., 2022). Information security policies are established in many organizations to protect their information systems. When interacting with these systems, employees are required to comply with certain rules and responsibilities that are formulated by the organization (Mehari, 2022). Therefore, it can be said that with the increasing reliance of organizations on cyber environments to manage their daily operations, information security protection behaviors in such environments have become a vital issue (Soliman & Mohammadnazar, 2022). Protecting information security requires a special system for protection, but users themselves also take reasonable protective measures and so on. The process of protecting information security requires a variety of strategies that are used together and used sensibly. Only in this way can the possibility of information security violations be minimized, and security guarantees can be obtained (Alshare et al., 2018).

Information security and network security are among these components that cannot be considered specific to a person or organization. New security problems always appear in information security, which require employees to pay attention and strengthen information security protective behaviors. In the big data environment, this data not only contains a lot of private information, but also contains a lot of business secrets. Therefore, for effective improvement, the comprehensive program must be updated from the perspective of security. Therefore, it is valuable to review the security and information protection measures of the computer network (Liu, 2021).

2.2 Organizational factors related to information security protective behaviors

Today, information security is a main focus and a vital aspect of all organizations as well as individual users (Mehari, 2022). In order to solve the problem of information security, the organization needs to use a wide range of knowledge, technology and organizational rules, and at the same time, it must be ensured that the organization is not only focused on technical solutions, but other key components of information security, including processes and employees (Boiko et al., 2019).

Many studies have focused on the relationship between information system employees and organizational information security and its effect on the level of protection, motivation, and subsequent behavior in the workplace. Effective information security also considers work-related efforts. Employees who have high organizational commitment continue to be members. Because the organization's values, goals, culture and initiatives are consistent with themselves. Similarly, employees with a positive emotional state have subjective values and satisfaction with performance in the organization and have a lower tendency to leave the service (Kim et al., 2020).

Commitment refers to the relative strength of a person's identity and involvement in a particular thing. Strong organizational commitment can be described as supporting the acceptance of the organization's goals and values. It is the desire to take serious actions on behalf of the organization and the desire to stay in the organization (Widodo & Damayanti, 2020).

On the other hand, job satisfaction is a personal characteristic, and it is an art that comes from fulfilling personal needs. Job satisfaction is all the factors of the job matrix that makes a person like his work situation and he wants to lead them without sorrow when starting daily work. Job satisfaction is a combination of the two words "satisfaction and job", the Merriam-Webster dictionary (2022) defines it as "an activity of satisfying or a state of pleasing" Job satisfaction is "the result of several situations in which the employee generally keeps his job in relation to the factors related to work and life". Job satisfaction is the emotional orientation that a person has towards his work, and it consists of two aspects: positive impact and negative impact (Said & El-Shafei, 2021).

Job satisfaction is known as a meaningful aspect of people's professional and private life, as well as an important field in the field of work (Bayrakdar & King, 2021). Job satisfaction is an important prerequisite for creating a suitable work environment (Ohara et al., 2021). This leads to the following hypothesis:

H1: Organizational commitment and job satisfaction have a significant effect on the motivation to protect information.

2.3 Protection motivation theory and factors extracted from it

Protection motivation theory was proposed by Rogers (1983) to explain how people process threats and choose responses to protect themselves in the context of health (Tang et al., 2021). According to the protection motivation theory, people respond to threats and protect themselves based on two processes: threat appraisal and coping appraisal. The threat assessment process evaluates the threat. Individuals evaluate proposed responses to threats at the same time as evaluating their own threat in a process called coping appraisal (Tang et al., 2021).

Fear is a mediating variable between perceived vulnerability and threat appraisal. Protection motivation is a mediating variable between stages of threat appraisal, coping appraisal and preventive behavior. Protection motivation is synonymous with behavioral intention and causes the behavior to be aroused or continued and is like an intermediate structure between the two stages of threat assessment and confrontation and protective behavior. In order to invoke protection motivation, perceived sensitivity and severity must overcome the rewards of the incompatible response and perceived self-efficacy must overcome the costs of the compatible response (Pratama et al., 2025). Studies in the field of this theory showed that the constructs of this theory are very important in predicting preventive behaviors (Jahani Eftekhari & Peyman, 2018). This leads to the following two hypotheses:

H2: Sensitivity to threat and intensity of threat have a significant effect on fear.

H3: Fear, self-efficacy and response cost have a significant effect on the motivation to protect information.

2.4 Theory of planned behavior and factors extracted from it

Ajzen presented the theory of planned behavior in 1985 due to the limitations in the theory of rational behavior. By adding a new factor to the theory of planned behavior, under the title of perceived behavioral control, he tried to cover the most important limitation of the theory of rational action. Like the theory of rational action, in the theory of planned behavior (which was formed with the development of the theory of rational action), the intention of people to perform a certain behavior is considered a key factor (Ohara et al., 2021).

The results reveal that self-efficacy, perceived vulnerability, and perceived severity significantly influence security behavior intention. Furthermore, threat awareness was identified as a significant predictor of response efficacy, perceived vulnerability, and self-efficacy. Security knowledge was found to play a crucial

role in shaping perceived severity, perceived vulnerability, and response efficacy. By fostering a culture of vigilance and improving employees understanding of the severity and vulnerability of phishing attacks, organizations can enhance their resilience against cyber threats and mitigate potential risks effectively (Pratama et al., 2025).

This behavioral theory summarizes that behavioral beliefs can lead to favorable or unfavorable attitudes and normative beliefs, which may lead to mental norms, and control beliefs may become perceived behavioral control (Rahman et al., 2022). The theory of planned behavior is developed for behaviors that are not sufficiently under a person's voluntary control. In this theory, which uses the perspectives of logical action and social learning, a person's decision to act (behavioral intention) is the most immediate and important predictor of behavior.

On the other hand, because not all behaviors are voluntary, the perceived behavioral control variable is also another predictor of behavior, since this theory is interested in understanding human behavior in addition to predicting behavior. Behavioral intention is determined with the help of three constructs-attitudes, mental norms and perceived behavioral control. That is, performing a behavior not only depends on the effort of the person to do it, but also the person's control over other factors such as necessary information, skills and abilities, etc. is also decisive (Afshani et al., 2020). This leads to the following hypothesis:

H4: Attitude, perceived behavioral control, mental norms have a significant effect on the motivation to protect information.

2.5 Motivation to protect information

Motivation indicates an internal desire to take action because it provides opportunities to satisfy needs and receive benefits in different ways (Kim et al., 2020). Motivation is an internal force and a factor in human behavior and helps to adapt and adapt to human life and influences behavior by directing attention. In the field of human behavior, there are factors that not only force people to act, but also lead them to a specific goal. Psychologists call these factors motivation. Motivation includes the internal state or pressure and the goal towards which the behavior is directed (Ohara et al., 2021). Incentives are those factors that make a person to do something. Incentives are rewards or generally stimuli that make the fire of a person's desire to satisfy their desires faster. At the same time, these factors are a means of establishing compatibility between different needs and even prioritizing a specific need. There are three general sets of motives: the motive of enjoyment (fun and escape from everyday life), the individual motive (success and belonging to the team) and the motive

of socialization (social and family interaction) (Rahman et al., 2022). According to the protection motivation theory, motivation is the intention to perform protective behavior against danger (Jahani Eftekhari & Peyman, 2018). This leads to the following hypothesis:

H5: the motivation to protect information has a significant effect on the protective behaviors of information security among the employees of the telecommunications company in Khuzestan region.

H6: subscales of job-related organizational factors, protective theory and planned behavior theory have a significant effect on information security protective behavior by mediating information protection motivation with information security protective behavior.

3. Methodology

3.1 Design

The current research is practical in terms of its purpose. The current research is descriptive according to the type of data collection. Also, this research is causal in nature, which aims to investigate the effect of variables on each other.

3.2 Participants

The statistical population studied in this research is all the employees of Khuzestan Telecommunications Company. The size of the community is equal to 1642 people. In order to estimate the sample size, Cochran's formula was used. Considering the number of samples, 450 questionnaires were distributed among the sample members, anticipating the possibility of not completing or handing in some of the questionnaires. Finally, 338 questionnaires were received, and 311 questionnaires were analyzed. The return rate of the questionnaire was 0.75. A non-random sampling method was also available. Before implementing the questionnaire, a pilot sample of 30 people was selected and evaluated to localize and validate this questionnaire in Iranian society.

3.3 Instrument

A questionnaire was used as a data collection tool. The questionnaire had 47 questions from Ma (2022) research. This questionnaire has 6 components. The components of job-related organizational factors (organizational commitment and job satisfaction), protection motivation theory (threat sensitivity, threat severity, self-efficacy and response cost), planned behavior theory (attitude,

perceived behavioral control and subjective norms). The independent variables are the fear component, the motivation to protect information as mediating variables, and information security protective behaviors as the criterion variable. This questionnaire was used from the five-choice Likert scale.

The 5-point Likert scale is widely used in research and surveys because of its simplicity and efficiency in collecting attitudinal data and opinions. By providing five response options (usually from "strongly disagree" to "strongly agree"), the scale allows respondents to express their opinions more precisely while also making it easier for researchers to analyze the data. In this study, the standard questionnaire of Ma (2022) was used, the validity of which was confirmed in the article by theorists and authors of the article.

3.4 Validity and reliability of measurement tools

In examining the convergent validity of the article, the mean variance extracted for all variables was found to be above 0.6, which is greater than 0.5, confirming the convergent validity. Also, in terms of divergent validity, the questionnaire questions were confirmed, and the correlation of the root-mean-square of the extracted variance was higher than all other cross-correlations.

In alignment with established PLS-SEM best practices, we evaluated our model using key metrics supported by foundational and contemporary literature. Convergent validity was confirmed using the Average Variance Extracted (AVE), with all constructs exceeding the recommended threshold of 0.50 (Fornell & Larcker, 1981). Internal consistency reliability was assessed via rho_A (ρ_a), with values above 0.70 indicating adequate reliability, consistent with Hair et al. (2019). The structural model's explanatory power was evaluated using the coefficient of determination (R2), interpreted following Chin's (1998) benchmarks, where values of 0.25, 0.50, and 0.75 represent weak, moderate, and substantial predictive relevance, respectively. Path significance was determined using bootstrapped p-values, with effects considered significant at $p < 0.05$ (Hair et al., 2019). Finally, discriminant validity was established via the Fornell–Larcker criterion, ensuring that the square root of each construct's AVE exceeded its inter-construct correlations (Fornell & Larcker, 1981). These rigorous assessments ensure our model adheres to current methodological standards in PLS-SEM research. In this study, Cronbach's alpha method was used to determine reliability. To calculate Cronbach's alpha coefficient, first the variance of the scores of each subset of the questionnaire questions and the total variance must be calculated. To check the validity and reliability of the questionnaire from varimax rotation, AVE, CR., and Cronbach's test were used, which is shown in Table 1.

Table 1. Factor loadings of indicators

Variable	Question	loadings	AVE	C. R.	Cronbach's alpha
Organizational commitment	q1	.821	.722	.912	.872
	q2	.825			
	q3	.897			
	q4	.853			
Job satisfaction	q5	.817	.571	.837	.740
	q6	.817			
	q7	.785			
	q8	.883			
Threat sensitivity	q9	.812	.709	.879	.797
	q10	.883			
	q11	.830			
Threat severity	q12	.850	.724	.887	.815
	q13	.893			
	q14	.807			
Self-efficacy	q15	.915	.816	.947	.926
	q16	.890			
	q17	.878			
	q18	.930			
Response cost	q19	.699	.626	.866	.786
	q20	.907			
	q21	.917			
	q22	.593			
Attitude	q23	.753	.683	.896	.846
	q24	.889			
	q25	.856			
	q26	.800			
Perceived behavioral control	q27	.832	.742	.896	.835
	q28	.878			
	q29	.875			
Subjective norms	q30	.911	.653	.848	.736
	q31	.815			
	q32	.862			

Variable	Question	loadings	AVE	C. R.	Cronbach's alpha
Fear	q33	.775	.579	.873	.821
	q34	.710			
	q35	.756			
	q36	.806			
	q37	.752			
Information protection motivation	q38	.787	.774	.945	.926
	q39	.887			
	q40	.926			
	q41	.916			
	q42	.875			
Information security protective behaviors	q43	.840	.802	.953	.938
	q44	.902			
	q45	.916			
	q46	.923			
	q47	.894			

3.5 Data analysis

Multivariate analysis refers to a series of analysis methods whose main feature is the simultaneous analysis of multiple independent variables with multiple dependent variables (Vinkenoog et al., 2023). The analysis was done using statistical software such as SPSS version 25, and for modeling and final analysis, SmartPLS version 3.3 software was used. In order to describe the findings, classify the groups in terms of various traits and describe the characteristics of the statistical population, the mean, frequency percentage, variance, standard deviation and other tests are used frequency tables and graphs to better describe the data from the central indices as well as dispersion indices.

4. Findings

It is shown in Table 2 in the preliminary survey regarding demographic characteristics.

According to Table 2, it can be seen that among the employees, 31.5% of the respondents are men and 68.5% are women. According to the results, the majority of society is made up of men. In particular, the level of education is 10.6 percent post-graduate, 60.8 percent bachelor's degree, 21.5 percent master's degree, and 1.7 percent Ph. D. Regarding age, 30.5% are less than 30 years old, 42.8% are 31 to 40 years old, 25.1% are 41 to 50 years old, and 1.6% are more than 50 years old.

Table 2. Frequency distribution of respondents' demographic characteristic

Category	Profile	Frequency	Percentage
Gender	Male	98	31.5
	Female	213	68.5
Age	⩽30	95	30.5
	31 - 40	133	42.8
	41 - 50	78	25.1
	⩾51	50	1.6
Degree of education	post-graduate	33	10.6
	Undergraduate	189	60.8
	Masters	67	21.5
	Ph. D.	22	7.1

4.1 Model fit

The goodness-of-fit index is calculated as the geometric mean of R^2 and the average of the commonality, as shown in Table 3.

Table 3. Goodness of Fit Validity Index (main research model)

Variable	Communality	R2	GOF
Organizational commitment	.520	-	.548
Job satisfaction	.324	-	
Threat sensitivity	.401	-	
Threat severity	.430	-	
Self-efficacy	.669	-	
Response cost	.397	-	
Attitude	.460	-	
Perceived behavioral control	.433	-	
Subjective norms	.320	-	
Fear	.371	.384	
Information protection motivation	.651	.667	
Information security protective behaviors	.693	.857	
Average	**.472**	**.636**	

The positiveness of the goodness of fit index shows the overall fit of the model. Because this value is equal to 0.548 and more than 0.4 for the main model, as a result, the overall fit of the models is confirmed.

4.2 Testing the main hypothesis using linear structured relationships

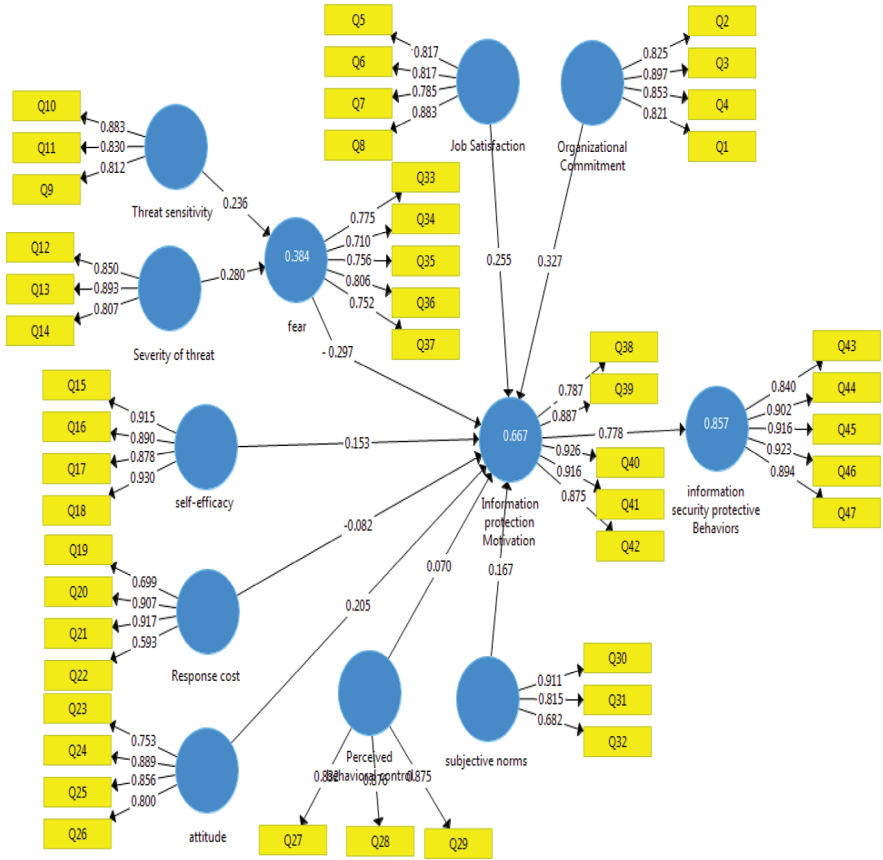
After determining the measurement models in order to evaluate the conceptual model of the research, as well as ascertaining the existence or non-existence of a causal relationship between the variables of the research and checking the appropriateness of the observed data with the conceptual model of the research, the hypotheses of the research using the model Structural equations were also tested. Based on the significance level of 0.05, the critical value must be greater than 1.96, the value of the parameter lower than this is not considered important in the model, and values smaller than 0.05 for the P-value indicate a significant difference in the value calculated for the weight-Regression values with zero value are at the 0.95 level. The general model and hypothesis testing results are presented in Figures 2 and 3.

4.3 Statistical analysis of the main research model

Path analysis method has been used to investigate the causal relationship between independent and dependent variables and verify the entire model. The path analysis in this research was done using the software of SmartPLS. The results of PLS outputs for the main hypothesis of the research are given below.

According to Table 4, the influence coefficient and t-statistic value of the variables' sensitivity to threat (β=0.236, t=3.138) and threat intensity (β=0.280, t=3.479) on fear, both of which are greater than it is 1.96. It can be concluded that threat sensitivity and threat severity have a significant effect on fear. Other variables include organizational commitment (β=0.327, t=5.365), job satisfaction (β=0.255, t=3.439), self-efficacy (β=0.153, t=2.947), Attitude variables (β = 0.205, t = 3.199) and subjective norms (β = 0.167, t = 2.989) on information protection motivation, all of which are greater than 1.96, which can be concluded that these variables have a significant effect on information protection motivation. But the response variables (β= -0.082, t = 0.434) and perceived behavioral control (β= 0.070, t = 0.469) had a significant effect on information protection motivation, which is smaller than 1.96. Did not have the effect coefficient and t-statistic value of the information protection motivation

Figure 2. General model measurement and hypothesis results in standard mode

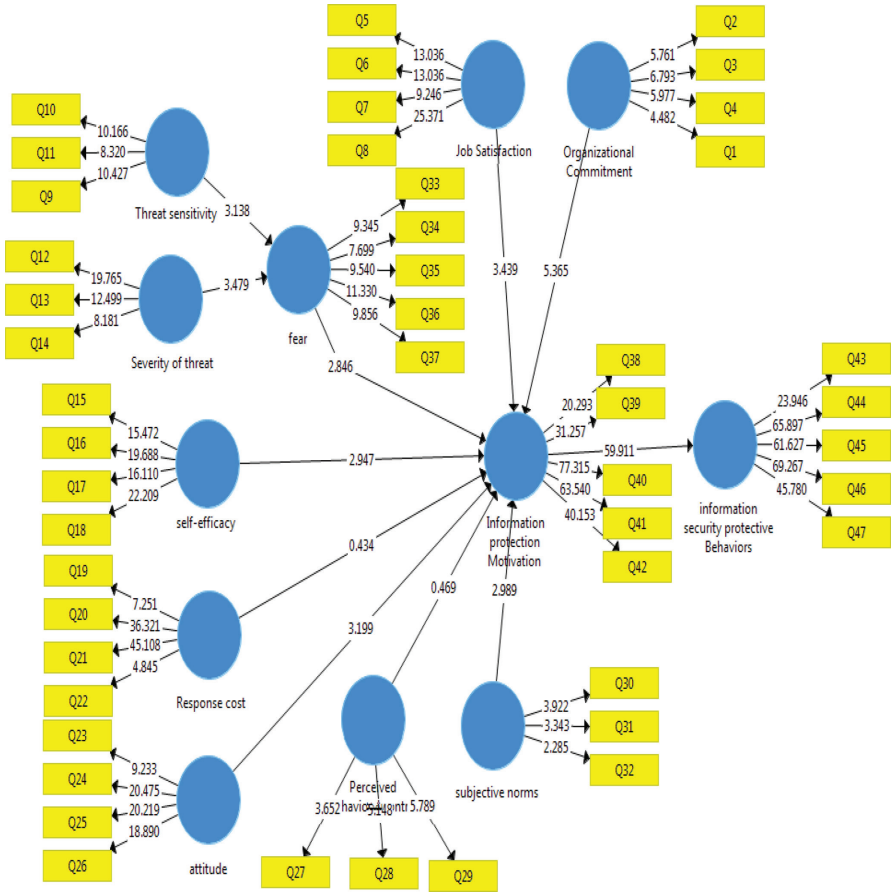


variable (β=0.778, t=59.911) have a significant effect on information security protection behaviors. The effect coefficient and t-statistic value of the fear variable (β=-0.297, t=2.846) have a significant effect on information protection motivation, which is greater than 1.96.

Sixth hypothesis: subscales of work-related organizational factors, protective and planned behavior theory have a significant effect on information security protective behavior by mediating information protection motivation with information security protective behavior. The results of this test are shown in Table 5.

According to Table 5, the results of the bootstrapping analysis show that the significance level for the full effect of the research variables is less than 0.05. In addition, the significance level for the indirect effect of all mediators, except the cost of responding and perceived behavioral control, is less than 0.05. As a result, eight hypotheses are confirmed and two hypotheses are rejected.

Figure 3. Measurement of the general model and the results of the hypotheses in a significant state



5. Discussion

The first hypothesis of the research was that organizational commitment and job satisfaction have a significant effect on the motivation to protect information among employees. The results of this research showed that organizational commitment and job satisfaction have a significant effect on the motivation to protect information among the employees of the telecommunications company in Khuzestan region. The obtained result is in line with the results of Safa and von Solms (2016) and Ma (2022). Organizational commitment refers to an employee's ability to identify and participate in his/her organization. Employees who are more involved with their organization are more likely to believe that their behaviors will be beneficial to their organization's performance and are

Table 4. The effect of organizational commitment and job satisfaction on information protection motivation

Hypothesis	Path			β	t-value	Result
H1	Threat sensitivity	→	Fear	.236	3.138	Confirmed
	Threat severity	→	Fear	.280	3.479	
H2	Organizational commitment	→	Information protection motivation	.327	5.365	Confirmed
	Job satisfaction	→	Information protection motivation	.255	3.439	
H3	Self-efficacy	→	Information protection motivation	.153	2.947	Confirmed
	Response cost	→	Information protection motivation	-.082	.434	Not confirmed
H4	Attitude	→	Information protection motivation	.205	3.199	Confirmed
	Perceived behavioral control	→	Information protection motivation	.070	.469	Not confirmed
	Subjective norms	→	Information protection motivation	.167	2.989	Confirmed
H5	Fear	→	Information protection motivation	-.297	2.846	Confirmed
	Information protection motivation	→	Information security protective behaviors	.778	59.911	Confirmed

more likely to be motivated to protect information. Since organizational commitment requires identification with an organization, therefore, evoking organizational commitment led to compliance with organizational rules and forced employees to support information security protection procedures. The results show that the organizational variable of organizational commitment strongly explains the motivation to protect information and positively affects the motivation to protect information. The path between organizational commitment and

Table 5. Investigating the mediating role of research variables

Hypothesis					Total Effect		Indirect		Result
					β	P- value	β	P- value	
Organizational commitment	→	Information protection motivation	→	Information security protective behaviors	.360	P<.05	.186	P<.05	Confirmed
Job satisfaction	→	Information protection motivation	→	Information security protective behaviors	.326	P<.05	.152	P<.05	Confirmed
Self-efficacy	→	Information protection motivation	→	Information security protective behaviors	.657	P<.05	.205	P<.05	Confirmed
Response cost	→	Information protection motivation	→	Information security protective behaviors	.342	P>.05	.071	P>.05	Not confirmed
Attitude	→	Information protection motivation	→	Information security protective behaviors	.421	P<.05	.326	P<.05	Confirmed
Perceived behavioral control	→	Information protection motivation	→	Information security protective behaviors	.355	P>.05	.029	P>.05	Not confirmed
Subjective norms	→	Information protection motivation	→	Information security protective behaviors	.432	P<.05	.302	P<.05	Confirmed
Threat sensitivity	→	Fear	→	Information protection motivation	.379	P<.05	.376	P<.05	Confirmed
Threat severity	→	Fear	→	Information protection motivation	.396	P<.05	.343	P<.05	Confirmed
Fear	→	Information protection motivation	→	Information security protective behaviors	.315	P<.05	.393	P<.05	Confirmed

motivation to protect information shows that the employees of the Khuzestan region telecommunication company tend to have more psychological investment in the organization and, as a result, have more commitment to spending extra time and effort to protect information assets. The obtained result is inconsistent with Ma research (2022). People with high job satisfaction pay more attention to organizational information assets. This issue is important for data security tasks in today's environment. The results of the research remind the managers of the organization to pay attention to the feelings of the employees, such as liking and enjoying the job (i. e. internal and external job satisfaction) in order to improve information security. It can be concluded that the key to encouraging information security protective behaviors from an organizational point of view is to increase the level of organizational commitment and job satisfaction of employees. These missing links in the information security chain are strong determinants for information protection motivation and actual information security protection behaviors. Establishing organizational commitment and job satisfaction among employees with the goal of organizational security is a fundamental matter. Because it requires not only satisfying the needs of employees (for example, work-life balance, reward and well-being) but also creating a pleasant and harmonious organizational atmosphere.

The second hypothesis of the research was based on the fact that threat sensitivity and threat intensity have a significant effect on fear among the employees of the telecommunication company in Khuzestan region. The results of the present study showed that sensitivity to threat and intensity of threat have a significant effect on fear among the employees of the telecommunication company in Khuzestan region. Regarding the result of sensitivity to threat and sourness, the obtained result is in line with the research of Ma (2022). Employees who experience strong feelings of fear as a result of threat appraisals will have stronger behavioral intentions and more actual protective behaviors. For example, targeted security education and training programs should reinforce the importance of protecting information security and define employee responsibilities for doing so. The employees of the telecommunications company consider threat sensitivity as a necessary factor and make them want to take security measures to protect the systems against data breaches. Previous studies confirm this issue and show that when organizational managers convey fear to employees, employees perceive their identity as protectors of organizational information security. Employees hide or take for granted the fear of information security, threat sensitivity and threat severity when they ensure that they meet specific security responsibilities.

The third hypothesis was that self-efficacy and response cost have a significant effect on the motivation to protect information among employees. The results of

this research showed that self-efficacy has a significant effect on the motivation to protect information among the employees of the telecommunications company in Khuzestan region. However, the cost of responding does not have a significant effect on the motivation to protect information among the employees of Khuzestan Telecommunication Company. Regarding the self-efficacy, it is in line with the research of Soheili et al. (2021), Tang et al. (2021) and Ma (2022). This factor emphasizes a person's ability or judgment about his abilities to cope or perform the recommended behavior. Self-efficacy emphasizes the abilities and competencies of a person to cope with information security protective behaviors. According to information security policies, it is expected that people with high security capabilities and competences understand the need to protect information more. It can be said that when the employees learn the information protection methods well and are confident of doing it correctly, their motivation to protect the systems against information breach will increase and they will take the necessary measures in this regard. In relation to the cost of response, the result obtained is inconsistent with the results of Soheili et al. (2021), Tang et al. (2021), and Ma (2022). Additionally, contrary to the result of this research, similar studies (Herath & Rao, 2009; Herath et al., 2014; Siponen et al., 2010) found the effects of response cost on the intention to comply with the policy of security policies. and also evaluated the behavioral intentions of users to use email authentication systems. For example, Herath et al. (2014) showed that the response cost of email screening has a significant negative effect on attitudes toward the perceived usefulness of email authentication, because the use of email security technology is a tedious process. It is a doer. A careful examination of the cognitive cost-benefits makes the perception of the cost of response. Therefore, it can be said that the employees of Khuzestan telecommunication company do not have much understanding of the cost and benefits of implementing the recommended protective behaviors, sacrificing time and effort, and incurring other costs to protect their organization's information. Thus, they do not make an effort to build stronger security defense systems to deal with information threats.

The fourth hypothesis: attitude, perceived behavioral control and mental norms have a significant effect on the motivation to protect information among the employees of the telecommunications company in Khuzestan region. The results showed that the attitude has a significant effect on the motivation to protect information among the employees of the telecommunication company in Khuzestan region. But the perceived behavioral control does not have a significant effect on the motivation to protect information among the employees of the Khuzestan telecommunications company. Regarding the attitude, the obtained result is in line with the research results of Safa and von Solms

(2016) and Ma (2022). Attitude is defined as a person's positive or negative feelings towards engaging in information protection procedures. People who have positive beliefs and values about the organization's information protection will have favorable tendencies to follow such laws, requirements and instructions. On the other hand, those who lack such favorable attitudes do not follow such behaviors easily. However, in relation to the perceived behavioral control, the obtained result is inconsistent with previous research in this area. Perceived behavioral control refers to a person's perceived ease or difficulty in performing or facilitating a specific behavior. A person with higher perceived behavioral control has the belief that he has the ability to perform a required action in the face of reasonable obstacles or facilitating conditions. One of the potential obstacles to data protection is that it is necessary to apply these measures not only to oneself but also to others. In current research, it seems that employees feel that they cannot control their colleagues in general with high self-efficacy. In this case (with respect to equal conditions), behavioral control will not have an effect on social interaction. And it will not motivate them. In relation to mental norms, the obtained results are in line with the results of the research of Safa and von Solms (2016) and Ma (2022). Mental norms describe a person's perception of what important people think about a certain behavior. In the field of information protection in organizations, employees are most likely to find the motivation to protect information when they realize that those around them, such as superiors, peers and subordinates, follow and obey such instructions. A plausible explanation for this finding is that the motivation to protect information can be influenced by the opinions and perceptions of peers and other influential people in one's immediate environment. Therefore, management can ensure the success of information protection motivation programs by identifying and assigning influential people in the organization who are able to motivate or shape the opinions of others to follow the information systems security policy in their fields.

Fifth hypothesis: The fear and motivation of information protection has a significant effect on information security protection behaviors among employees. It can be concluded that the fear and motivation of information protection has a significant effect on information security protection behaviors among the employees of the Khuzestan telecommunications company. Based on the protection motivation theory, this study confirmed that fear increases the willingness to participate in protective security measures as well as actual protective behaviors. This is consistent with previous studies showing that fear has a significant impact on employee safety motivations, intentions, and behaviors (Abd Latif et al., 2025).

If the threat assessment messages do not lead to the perception of fear, employees will be less aware of the importance of their role in protecting information security against threats. The lack of widespread use of fear may be a problematic omission in information security studies. Ignoring the consequences of fear may lead to potentially spurious and misleading results that undermine research findings. However, regarding the motivation to protect information, the available literature in this field fully supports this finding, and this finding is consistent with the findings of Soheili et al. (2021) and Ma (2022). The motivation of a person's desire and feeling is to make extra efforts to achieve and guide a behavior. The motivation to protect information security is essential in achieving the goal of improving these behaviors as well as stimulating protective measures. Johnston and Warkentin (2010) claimed that when the threat evaluation and coping evaluations are at a moderate to high level, individual protection motivation increases equally and, therefore, in the behavior it really affects. When the employees have the motivation to carry out countermeasures and are not indifferent in order to successfully prevent the threats related to the information security violation of the organization, they automatically look for solutions and try as much as possible. May they use the facilities of the organization.

Sixth hypothesis: subscales of job-related organizational factors, protective theory and planned behavior theory have a significant effect on information security protective behavior by mediating information protection motivation with information security protective behavior among employees.

5.1 Conclusion

This study sheds light on how psychological and organizational factors intersect to shape information security behaviors among employees. By applying PMT and the TPB, the research offers a nuanced understanding of how internal states, such as fear and motivation, can influence practical actions within a workplace setting. It confirms that simply establishing policies is not enough; the success of those policies hinges on how employees perceive threats and how motivated they are to act against them. Organizational commitment and job satisfaction emerged as strong motivators for information security compliance. Employees who feel valued and aligned with their company's mission are more likely to protect its digital resources. This insight calls for a cultural shift in management strategies, from purely technical solutions to a more people-centered approach. Enhancing job satisfaction and reinforcing organizational loyalty can, in effect, become a frontline defense against cyber threats.

Fear also plays a crucial role in shaping behavior. When employees are made aware of the severity and likelihood of threats, their emotional response can prompt them to take protective measures more seriously. This highlights the importance of effective communication and awareness training that does more than inform, it should also engage emotionally. Fear, when balanced with clear and empowering messaging, can motivate rather than paralyze.

Furthermore, the study reveals that attitudes, perceived norms, and self-efficacy are more influential than control or cost-related perceptions. Employees are more driven by belief in their own capabilities and by the influence of respected peers or leaders than by logistical concerns. This suggests that cultivating a supportive social environment, where secure behavior is visibly practiced and reinforced, could significantly elevate security outcomes. In conclusion, the findings underscore the importance of treating employees not as passive rule-followers but as active partners in information security. A strategy that prioritizes human behavior, shaped by motivation, emotion, and shared values, is likely to be far more sustainable and effective. For organizations like the Khuzestan Telecommunications Company, investing in employee experience and fostering a security-conscious culture may be the most impactful way forward in an era of escalating digital threats.

5.2 Limitations and suggestions for further research

While this study offers valuable insights into the behavioral factors influencing information security practices, it is not without limitations. The use of non-random, convenience sampling limits the generalizability of the findings beyond the specific context of Khuzestan Telecommunications Company, Iran. Moreover, relying solely on self-reported data through a questionnaire may introduce biases such as social desirability or inaccurate self-assessment. The cross-sectional nature of the study also restricts the ability to establish causal relationships over time, making it difficult to assess the long-term consistency of the observed behaviors. Future research should aim to expand the scope by including multiple organizations across different industries and regions to enhance external validity. Longitudinal studies could better capture how protection motivation and security behavior evolve in response to policy changes or cyber incidents. Additionally, integrating qualitative methods such as interviews or focus groups may help explore deeper psychological drivers and organizational dynamics that quantitative tools may overlook. Finally, testing this model in other cultural contexts could reveal how national or organizational culture interacts with security behavior, offering a more comprehensive global understanding.

References

Abd Latif, S. F., Sulaiman, N. S., Abd Aziz, N. S., Yacob, A., & Nasir, A. (2025). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science & Applications, 16*(3). https://doi.org/10.14569/ijacsa.2025.01603117

Afshani, S. A., Ruhani, A., & Abdinejad, A. (2020). Experimental Application of Planned Behavior Theory in Explaining the behavior of keep up with the Joneses of Married Women in Yazd. *Quarterly of Social Studies and Research In Iran, 9*(2), 315–342. https://doi.org/10.22059/jisr.2020.294632.984

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of Applied social Psychology, 32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity, 11*(1), 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information & Computer Security, 26*(1), 91–108.

Bayrakdar, S., & King, A. (2021). Job Satisfaction and Sexual Orientation in Britain. *Work, Employment and Society*, 1–19. https://doi.org/10.1108/ics-09-2016-0073

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia Computer Science, 149*, 65-70. https://doi.org/10.1016/j.procs.2019.01.108

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

Chang, A. J. T., Wu, C. Y., & Liu, H. W. (2012). The effects of job satisfaction and organization commitment on information security policy adoption and compliance. In *IEEE International Conference on Management of Innovation & Technology (ICMIT)*, 442–446. IEEE. https://doi.org/10.1109/icmit.2012.6225846

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based

on social control and deterrence theory. *Computers & Security*, *39*(Part B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Chin, W. W. (1998). The Partial Least Squares approach to structural equation modelling. In: Marcoulides, G. A. (Ed.), *Modern methods for business research* (p. 295–336). Lawrence Erlbaum

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312

Giao, H. N. K., Vuong, B. N., & Duy Tung, D. (2020). A model of organizational culture for enhancing organizational commitment in telecom industry: Evidence from vietnam. *WSEAS Transactions on Business and Economics, 17*, 215–224. https://doi.org/10.37394/23207.2020.17.23

Hair, J., Hult, T., Ringle, C., Sarstedt, M., Castillo, J., Cepeda, G., & Roldán, J. (2019). Manual de partial least squares structural equation modeling (PLS-SEM). SAGE Publishing. https://doi.org/10.3926/oss.37

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1). https://doi.org/10.1111/j.1365-2575.2012.00420.x

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

Jahani Eftekhari, M., & Peyman, N. (2018). The Effect of educational intervention based on protection motivation theory on promoting pediculosis preventive behaviors among elementary school girls in Neyshabu. *Journal of Education and Community Health, 5* (2), 45–52.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566. https://doi.org/10.2307/25750691

Kim, J., Eys, M., Robertson-Wilson, J., & Dunn, E. (2019). Subjective norms matter for physical activity intentions more than previously thought:

Reconsidering measurement and analytical approaches. *Psychology of Sport & Exercise, 43*, 359–367. https://doi.org/10.1016/j.psychsport.2019.04.013

Kim, S., & Choi, M. (2002). Educational requirement analysis for information security professionals in Korea. *Journal of Information Systems Education, 13*(3), 237–248. https://aisel.aisnet.org/jise/vol13/iss3/11

Kim, S., Morgan, A., & Assaker, G. (2020). Examining the relationship between sport spectator motivation, involvement, and loyalty: A structural model in the context of Australian Rules football. *Sport in Society*, 1–28. https://doi.org/10.1080/17430437.2020.1720658

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*(2), 337–359. https://doi.org/10.1108/intr-07-2014-0173

Liu, C. J. (2019). Expectation, commitment, and charitable giving: The mediating role of trust and the moderating role of social status. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations, 30*(4), 754–767. https://doi.org/10.1007/s11266-018-0014-y

Liu, S. (2021). Computer network information security and protection measures under the background of big data. *Journal of Physics: Conference Series, 1881*(3), 032092. https://doi.org/10.1088/1742-6596/1881/3/032092

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, 59(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

Mehari, A. (2022). Personality difference associated with the information security performance of employees' in the Information Network Security Agency (INSA). *Research on Humanities and Social Sciences, 12*(1), 1–11.

Mojisola, F. O., Misra, S., Febisola, C. F., Abayomi-Alli, O., & Sengul, G. (2022). An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). *Egyptian Informatics Journal, 23*(2), 291–301. https://doi.org/10.1016/j.eij.2022.02.001

Ohara, Y., Nomura, Y., Yamamoto, Y., Okada, A., Hosoya, N., Hanada, N., ... & Takei, N. (2021). Job attractiveness and job satisfaction of dental hygienists: from Japanese dental hygienists' survey 2019. *International Journal of Environmental Research and Public Health, 18*(2), 755. https://doi.org/10.3390/ijerph18020755

Plachkinova, M., & Maurer, C. (2018). Security breach at Target. *Journal of Information Systems Education, 29*(1), 11–20. https://aisel.aisnet.org/jise/vol29/iss1/7

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Pratama, O., Aladin, R. A., Lim, B., & Sundjaja, A. M. (2025). Determinants of security behavior intention in state-owned enterprises: Applying protection motivation theory to phishing emails. *International Journal of Safety & Security Engineering, 15*(3). https://doi.org/10.18280/ijsse.150304

Rahman, F., Mahmud, I., Jiang, B., & Sarker, K. (2022). Extending the theory of planned behavior: a case of learning Chinese as a third language. *International Journal of Instruction, 15*(1), 945–964. https://e-iji.net/ats/index.php/pub/article/view/484

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153–176.

Safa, N. S., & Ismail, M. A. (2013). A customer loyalty formation model in electronic commerce. *Economic Modelling, 35*, 559–564. https://doi.org/10.1016/j.econmod.2013.08.011

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

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

Said, R. M., & El-Shafei, D. A. (2021). Occupational stress, job satisfaction, and intent to leave: nurses working on front lines during COVID-19 pandemic in Zagazig City, Egypt. *Environmental Science and Pollution Research, 28*, 8791–8801. https://doi.org/10.1007/s11356-020-11235-8

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

Soheili, F., Rostaei, R., Khasseh, A. A., & Shahbazi, M. (2021). Evaluating the behavior of users of mobile electronic devices with the emphasis on protection motivation theory of data breach: a case study of graduate

students. *Iranian Research Institute for Information Science and Technology, 36* (4), 1137–1157. https://doi.org/10.52547/jipm.36.4.1137

Soliman, W., & Mohammadnazar, H. (2022). New insights into the justifiability of organizational information security policy noncompliance: A Case Study. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. University of Hawai'i at Manoa. https://doi.org/10.24251/hicss.2022.823

Sommestad, T., Karlz´en, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *The Journal of Computer Information Systems, 59*(4), 344–353. https://doi.org/10.1108/ics-04-2014-0025

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly, 38*(2), 101572. https://doi.org/10.1016/j.giq.2021.101572

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC), 24*(1), 21–41. https://doi.org/10.4018/joeuc.2012010102

Vinkenoog, M., de Groot, R., Lakerveld, J., Janssen, M., & van den Hurk, K. (2023). Individual and environmental determinants of serum ferritin levels: A structural equation model. *Transfusion Medicine, 33*(2), 113–122. https://doi.org/10.1111/tme.12902

Widodo, W., & Damayanti, R. (2020). Vitality of job satisfaction in mediation: the effect of reward and personality on organizational commitment. *Management Science Letters, 10*(9), 2131–2138. https://doi.org/10.5267/j.msl.2020.1.016

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: an empirical analysis. *The Electronic Library, 35*(6), 1177–1190. https://doi.org/10.1108/el-09-2016-0183