

# Cracking the Code: A Comprehensive Analysis of Information Security Strategies Among Professionals

Abdullah Almuqrin, King Saud University, Saudi Arabia\*

 <https://orcid.org/0000-0002-6692-9694>

Ibrahim Mutambik, King Saud University, Saudi Arabia

 <https://orcid.org/0000-0001-6819-5244>

Justin Zuopeng Zhang, University of North Florida, USA

 <https://orcid.org/0000-0002-4074-9505>

Hashem Farahat, King Saud University, Saudi Arabia

Zahyah H. Alharbi, King Saud University, Saudi Arabia

 <https://orcid.org/0000-0003-3363-5005>

## ABSTRACT

With the expanding reach of the Internet of Things, information security threats are increasing, including from the very professionals tasked with defending against these threats. This study identified factors impacting information security behavior among these individuals. Protection motivation theory and the theory of planned behavior were employed along with work-related organizational factors as a theoretical framework. Data were collected through a survey of 595 information security professionals working in Saudi information technology companies. Structural equation modeling was used to analyze the data. Threat susceptibility, threat severity, self-efficacy, response cost, fear attitude, behavioral control, subjective norms, and organizational commitment were found to play a significant role in information security protection motivation and behavior, while job satisfaction did not.

## KEYWORDS

Attitude, Behavioral Control, Coping Appraisal, Information Security Behavior, Organizational Commitment, Protection Motivation Theory, Subjective Norms, Theory of Planned Behavior, Threat Appraisal

Due to the prevalence of emerging technologies such as the internet of things and cloud computing, many organizations adopt digital solutions. This digital transformation allows these organizations to improve their business processes and operations (Saeed et al., 2023). However, the main drawback of this transformation is privacy and information-security threats and breaches, posing a significant challenge that should be effectively addressed (Cai et al., 2023; Malik et al., 2022; Ataei Nezhad et al.,

DOI: 10.4018/JOEUC.345933

\*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

2022). Information is a valuable asset, and securing this asset can make a difference in the development of these organizations (Yeng et al., 2021). However, one of the key sources of information-security breaches is the human factor, including security professionals (Hughes-Lartey et al., 2021; Malik et al., 2022).

Security specialists are responsible for securing an organization's network infrastructure (Pearson, 2021). However, security breaches are sometimes caused by these same professionals. For example, a system administrator who had worked for 15 years at a paper mill in Port Hudson, Louisiana, was fired after being made redundant and used login credentials to get access to the mill's servers (Irwin, 2022). He changed the control systems, creating delays costing the company \$1.1 million in damages for missed deadlines. Clearly, such conduct can lead to reputational damage, huge financial losses, and claims for violating personal privacy. Therefore, to gain a better understanding of how information-security specialists carry out protective measures, extensive research is required to explore the factors influencing their behavior (Pearson, 2021). Previous studies have shown that formal sanctions alone against unwarranted and careless information-security behaviors do not necessarily lead to higher compliance (Al-Qirim et al., 2022; Chen et al., 2018; Wiafe et al., 2020).

In particular, data breaches within organizations have a huge impact on information security (Liang et al., 2022; Raimundo & Rosário, 2022) since the data often include direct identifiers such as name, date of birth, and address (Avraam et al., 2022), in addition to organizational information such as trade secrets and financial data (Yeng et al., 2021). Therefore, managing access to such data is a challenge (Raimundo & Rosário, 2022). Cross-system protection can be ensured when information-security professionals take privacy threats and vulnerabilities seriously and find effective methods for avoiding weaknesses (Malik et al., 2022). Accordingly, effort is required from the experts responsible for collecting, analyzing, and using data (Malik et al., 2022; Yeng et al., 2021). Therefore, organizations should focus on behavior to minimize these security risks (Bolek et al., 2023; Wall et al., 2022).

In 2022, Saudi information-technology enterprises generated US\$24.62 billion. This amount is expected to grow to US\$43.13 billion by 2027 with a compounded annual growth rate of 11.87%. However, the cumulative revenue for information-technology companies in Saudi Arabia is expected to be US\$195.96 billion between 2022 and 2027 (GlobalData, 2023). Nevertheless, little research has been conducted on information-security protection in developing countries such as Saudi Arabia. Since most of these studies have focused on organizations in developed countries, it remains to be seen how far their findings are relevant to Saudi Arabia, a country with a different cultural and institutional background. The present study sought to bridge this gap by identifying key factors influencing this behavior in Saudi Arabia.

## **THEORETICAL FRAMEWORK AND LITERATURE REVIEW**

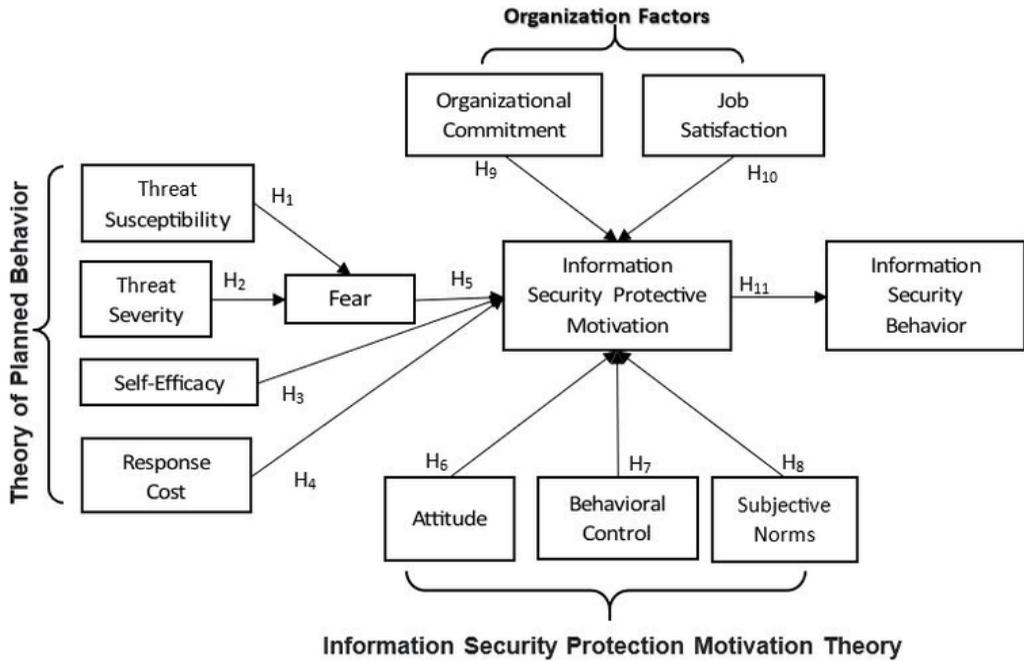
This study proposes a theoretical framework based on the constructs of protection-motivation theory, the theory of planned behavior, and two organizational factors to analyze their impact on the information-security behavior of experts. The framework and its associated hypotheses are present in Fig. 1 and explored in the following subsections. This approach was tested in a Saudi organizational setting to answer two research questions:

1. What factors significantly influence the behavior of Saudi information-security experts?
2. To what degree do these factors influence the behavior of Saudi information-security experts?

### **Protection-Motivation Theory**

Protection-motivation theory is used to predict and explain behaviors and how they induce noncompliance with security policies (Marshall et al., 2022). The theory describes the changes in an individual's attitude and behavior as a consequence of being exposed to a threat (Rogers, 1975,

Figure 1. Proposed Framework



1983). The protection motivation (i.e., behavioral intention) is created through an individual's threat and coping evaluations and appraisals when experiencing threatening circumstances (Rogers, 1983).

Many studies of protection-motivation theory have focused on the components of fear and fear appeals, while other components have not been explored in information-security research (Haag et al., 2021). The theory has been used in research to determine the factors that can improve individuals' security behavior and security outcomes in organizations (Wall et al., 2022) and the level of employees' information security policy compliance (Ajmi et al., 2019; Hanus & Wu, 2016; Ifinedo, 2012; Menard et al., 2018; Sommestad et al., 2019; Wang et al., 2023).

As such, this theory is based mainly on factors of threat appraisal and coping appraisal. Threat appraisal consists of two constructs: threat susceptibility, the degree to which an individual feels vulnerable to a threat, and threat severity, the degree to which the threat is perceived to be severe (Rogers, 1983). In this study, threat susceptibility represented the belief of the information-security professionals that their organization was vulnerable to a given threat, while threat severity was the degree to which they felt this threat could lead to extreme danger.

Fear is a negative emotional response that arises when we believe there is a threat that could cause harm. The level of fear we experience is determined by the susceptibility and severity of the predicted threat. This led to the following hypotheses:

**H<sub>1</sub>**: Threat susceptibility to information security has a positive effect on fear.

**H<sub>2</sub>**: Threat severity to information security has a positive effect on fear.

Coping appraisal refers to assessing the capability of an individual to avoid and cope with threats, with the aim of averting a given hazard (Haag et al., 2021; Rogers, 1983). The two factors associated with coping appraisal are self-efficacy and response cost. Self-efficacy is the confidence

an individual can perform a protective behavior toward information security (Ezati Rad et al., 2021; Haag et al., 2021; Kumar et al., 2023; Maddux & Rogers, 1983; Marikyan & Papagiannidis, 2023). Employing protection-motivation theory and the theory of planned behavior, Marshall et al. (2022) found that self-efficacy had a significant direct impact on security-behavior intention and an indirect impact on security behavior among university students. Response cost is the estimated physical and psychological cost (e.g., in time, money, and effort) of performing a protective behavior (Ezati Rad et al., 2021; Jayawardena et al., 2023; Taheri-Kharameh et al., 2020), overcoming a complex problem, or controlling a powerful habit (Haag et al., 2021). Both self-efficacy and response cost have a great impact on behavioral intention (Farooq et al., 2019; Hsu & Lee, 2023; Lee & Seomun, 2021; Maddux & Rogers, 1983; Marikyan & Papagiannidis, 2023; Marshall et al., 2022). Hence, the following hypotheses were proposed:

**H<sub>3</sub>**: Self-efficacy has a positive effect on information-security protection motivation.

**H<sub>4</sub>**: Response cost has a negative effect on information-security protection motivation.

Fear can have a significant mediating effect on protection motivation according to some researchers (e.g., Haag et al., 2021; Kim et al., 2022; Lin & Zhu, 2023; Maddux & Rogers, 1983; Marshall et al., 2022; Rogers, 1975, 1983) but not to others (e.g., Ifinedo, 2012; Lee & Seomun, 2021; Menard et al., 2018; Mutambik et al., 2023a; Oakley et al., 2020), although it is a main component of protection-motivation theory in theoretical reviews (e.g., Haag et al., 2021; Maddux & Rogers, 1983; Marikyan & Papagiannidis, 2023; Milne et al., 2000). In Kim et al. (2022), fear was found to significantly mediate the relationship between (a) local support, hygienic behavior, and conscious consumption and (b) perceived threat and response efficacy. Hanus and Wu (2016) revealed that high levels of fear could be induced by increasing threat vulnerability; however, it was not enough to use fear appeal to motivate desktop users to act on security threats. Hence, fear plays a crucial role in the cognitive mediating process and how information is processed. According to protection-motivation theory, fear acts as a moderator between threat appraisal and information-security protection motivation (Haag et al., 2021). Studies have shown that inducing fear in employees can increase their willingness to take protective measures (e.g., Hanus & Wu, 2016; Mutambik et al., 2023b; Oakley et al., 2020; Rogers, 1975). Accordingly, the following hypothesis was posited.

**H<sub>5</sub>**: Fear has a moderating effect on the relationship between information-security threat appraisal, represented in threat susceptibility and severity, and information-security protection motivation.

## Theory of Planned Behavior

The theory of planned behavior is also used to predict information-security behavior (Ajzen, 1991, 2020; Ali et al., 2021; Ifinedo, 2012). While prior research has attempted to combine both theories (e.g., Farooq et al., 2019; Gaurav & Panigrahi, 2022; Ifinedo, 2012; Lee & Seomun, 2021), few studies have tackled factors that can significantly influence the behavior of information-security professionals regarding information-security protection.

Empirical research has shown that the theory of planned behavior supports a wide range of behaviors (Yang & Xu, 2021). Thus, it is commonly used in information-systems research to predict and analyze different forms of behavior (Mutambik et al., 2023d; Sommestad et al., 2019; Zhang et al., 2020). Communication with others in organizations can affect people's feelings, responses, and behaviors. According to this theory, behavior is thus influenced by a set of beliefs that fall into three categories: attitudes, perceived behavioral control, and subjective norms (Ajzen, 1991, 2020; Ali et al., 2021; Sommestad et al., 2019; Venkatesh et al., 2003; Zhang et al., 2020).

A person's attitude is evaluated as the positive or negative feelings toward performing a behavior (Fishbein & Ajzen, 1975). In Zhang et al. (2020), attitude increased the behavioral intention to use a

mobile health service. In addition, attitude toward security-related behavior is related to organizational culture that can enforce and motivate a security behavior if the culture emphasizes its importance (Lin & Luo, 2021). Based on this, the following hypothesis was posited:

**H<sub>6</sub>:** Attitude toward information-security protection has a positive impact on information-security protection motivation.

Behavioral control is to what degree one can perform a behavior that is under one's control (Ajzen, 2020) and can influence a person's own confidence about intentions and related actions (Almuqrin et al., 2023a; Vafaei-Zadeh et al., 2019; Venkatesh & Davis, 2000). Safa and Von Solms (2016) found that information-security knowledge sharing significantly increased with behavioral control. In contrast, Tan et al. (2022) found no direct relationship between behavioral control and behavior intention among students after a campus security-preparedness exercise in universities in Malaysia. Behavioral control was investigated in the present study using the following hypothesis:

**H<sub>7</sub>:** Perceived behavioral control has a positive impact on information-security protection motivation.

Subjective norms are a person's perceptions of others' opinions about a behavior that should be performed by that person (Fishbein & Ajzen, 1975). In Vafaei-Zadeh et al. (2019), subjective norms were a significant factor in students' intention to use anti-malware recommended by security professionals. In organizations, subjective norms represent social power and pressure to perform or not perform a behavior (AlGhamdi et al., 2022). Information-security experts are exposed to the pressure of their leaders and managers who regard information-security protection motivation as vital. Subjective norms were examined in this study using the following hypothesis:

**H<sub>8</sub>:** Subjective norms have a positive impact on information-security protection motivation.

## **Work-Related Organizational Factors**

Individual as well as organizational factors impact security performance and the desire to protect information-system resources. Studies have shown that job satisfaction (e.g., Hughes-Lartey et al., 2021; Lee & Seomun, 2021; Li et al., 2022) and organizational commitment (e.g., Liu et al., 2020, 2022) are significant factors in this regard (Chang et al., 2012; Spector, 1985). Strong commitment makes employees more likely to stay in their organization, because they share the same beliefs, goals, culture, and initiatives as the organization (Almuqrin et al., 2023b; Lin & Luo, 2021; Meyer et al., 1993; Zhen et al., 2020). Additionally, employees who are passionate about and satisfied with their job are less likely to want to leave or harm it (Guzmán et al., 2018; Zhen et al., 2020). In this study, job satisfaction and organizational commitment are discussed as work-related organizational factors.

### ***Organizational Commitment***

Organizational commitment is "a psychological state that (a) characterizes the employee's relationship with the organization and (b) has implications for the decision to continue or discontinue membership in the organization" (Meyer & Allen, 1991, p. 67). Employees' organizational commitment refers to their loyalty, obligation, and desire to achieve organizational objectives (Meyer & Allen, 1997). It creates a bond between employees and their organization, which makes them feel that the organization's goals and values are their own. Employees who have a strong commitment to their organization are likely to react differently to information-security threats that affect the organization compared to those who have less commitment (Liu et al., 2020, 2022; Oz, 2001; Posey et al., 2015). This factor can predict levels of protective motivation, indicating information-security professionals are equipped to handle threats. The factor was explored with the following hypothesis:

**H<sub>9</sub>**: Organizational commitment has a positive impact on information-security protection motivation.

### *Job Satisfaction*

Job satisfaction is a “positive emotional state resulting from the evaluation of one’s work and professional experience” (Locke, 1976, p. 1304). Employees’ job satisfaction involves a variety of intrinsic and extrinsic factors that contribute to their feelings of satisfaction. Intrinsic factors include the nature of the work, recognition, and autonomy, while extrinsic factors include salary, supervision, working conditions, benefits, and job security (Baroudi et al., 2022; Ennida & Allouani, 2023). Job satisfaction is a crucial factor in motivating employees to embrace organizational goals, maintaining morale, and contributing to employee well-being and work stability. It can motivate employees to consider and protect their organization’s information security (Alaidaros & Albeedh, 2022; Bascomb, 2020). Accordingly, the following hypothesis was explored:

**H<sub>10</sub>**: Job satisfaction has a positive impact on information-security protection motivation.

In this study, protection motivation was extended to include real protection behavior influenced by threat and coping appraisals. In contrast, some studies have focused on protection motivation, ignoring the relationship between motivation and actual behavior (Ifinedo, 2012; Mutambik et al., 2023c; Wall et al., 2022). Since the ultimate goal of such research is to enhance individuals’ information-security behavior, not simply improve their intentions, it is important to consider real actions and behavior. Hence, the following hypothesis was postulated:

**H<sub>11</sub>**: Information-security protection motivation has a positive effect on information-security behavior.

## **METHODOLOGY**

### **Instrument**

Table 1 depicts all constructs used in the study, along with the number of items in each construct and their sources.

Data was collected through an online questionnaire in Google Forms developed from validated scales in the literature with slight modifications. The items were examined for readability, consistency, and clarity by a panel of information-security experts. The items aimed to address the relationships between constructs that lead to positive information-security protection behavior. A pilot study was conducted with 23 information-security professionals in a well-known Saudi organization. All items used a 5-point Likert scale ranging from *strongly agree* to *strongly disagree*. The pilot study showed no anchoring bias in the survey design. This study contained 47 items, and therefore a 5-point Likert scale was suitable to use because it was easier to capture the opinions of the respondents and help them deliver reliable data without distortion or wasting much time and effort. A higher than 5-point scale would be boring for respondents and could cause distortion. Moreover, a reasonable number of respondents participated in the pilot study, which indicates that the 5-point Likert scale was a good choice for them. Moreover, the questionnaire was offered by the Saudi Open Data Portal and included everything related to the constructs.

### **Data Collection**

The link to the survey was made available to respondents from the investigated Saudi organizations from October to November 2023 through WhatsApp, LinkedIn, and Facebook. Bos (2020) argues that when research studies are conducted, ethics should be considered through protecting the rights, interests, confidentiality, and anonymity of participants and informing them about the possible risks

Table 1. Definition of Constructs

Construct	Definition	Items	Reference
Threat Susceptibility	How personally susceptible an individual feels to the communicated threat	3	Milne et al. (2000, p. 108)
Threat Severity	How serious the individual believes that the threat would be to his or her life	3	Milne et al. (2000, p. 108)
Self-Efficacy	The perceived ability of the person to actually carry out the adaptive (coping) response	4	Floyd et al. (2000, p. 411)
Response Cost	Any costs (e.g., monetary, personal time, effort) associated with taking the adaptive coping response	4	Floyd et al. (2000, p. 411)
Fear	A negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically	6	Boss et al. (2015)
Attitude	An individual's positive or negative feelings (evaluative affect) about performing the target behavior	4	Fishbein & Ajzen (1975, p. 216)
Behavioral Control	The perceived ease or difficulty of performing the behavior	2	Ajzen (1991, p. 183)
Subjective Norms	People's perception that most people who are important to them think they should or should not perform the behavior in question	3	Fishbein & Ajzen (1975, p. 302)
Organizational Commitment	A psychological state that (a) characterizes the employee's relationship with the organization and (b) has implications for the decision to continue or discontinue membership in the organization	4	Meyer & Allen (1991, p. 67)
Job Satisfaction	A pleasant or positive emotional state resulting from the evaluation of one's work and professional experience	4	Locke (1976, p. 1304)
Information-Security Protection Motivation	An intervening variable that arouses, sustains, and directs activity to protect the self from danger	5	Maddux & Rogers (1983, p. 470)
Information-Security Behavior	Peoples' actions they take to mitigate information-security threats	5	Tang et al. (2021)

they may encounter. Therefore, this study ensured the confidentiality and anonymity of its participants. An informed consent was obtained from each participant, and their privacy was protected at all times. Recruitment was through opportunistic and snowball sampling, which made it possible to reach a large sample. Opportunistic or convenience sampling was utilized in this study for recruiting the available information-security professionals from a few Saudi information-technology companies. The researcher was able to visit some of the information-technology companies, and with the help of their top management, a meeting was conducted with the information-security professionals, who were enthusiastic to share in this study. Moreover, to increase the number of participants, referrals were initiated using snowball sampling, and potential participants were approved to talk to other information-security professionals from other companies, who then contacted the researcher and showed a desire to participate in this study. Therefore, opportunistic and snowball sampling were effective in this study, and it was able to glean a large number of participants. These participants included information-technology and -security managers and other information-technology staff members. The sample contained 754 respondents, 595 of which (78.9%) gave complete responses and were accepted for data analysis. Respondent demographics are given in Table 2.

Table 2. Respondent Demographics

Item	Value	Percent
Average Age	34	
Gender	Male Female	61.5% 38.5%
Education Level	High school Bachelor's Master's PhD	5.1% 68.3% 23.96% 2.64%
Size of Organization	20 or below 21–50 51–100 Above 100	20.5% 48.8% 25.6% 5.1%
Work Experience	1 year or less 1–3 years 3–5 years Over 5 years	15.8% 20.6% 33.9% 29.7%

## Data Analysis

The proposal of Anderson and Gerbing (1988) was followed, based on a two-step strategy. The first step involved completing a measurement model analysis to assess the validity and reliability of the constructs. The second step was analyzing the structural links among the implicated latent variables. This ensured that the measurements were trustworthy before using them in the investigation. Once the validity and reliability of the measurements were examined, the structural model estimations using coefficients of determination ( $R^2$  values) and the importance of the path coefficients were determined. The structural equation modeling (SEM) utilized in this study is a sophisticated estimating technique capable of investigating the correlations between variables, whether dependent or independent. SEM is used to assess how different indicators contribute to the predicted latent constructs, which is known as the measurement model. It is also used to examine the relationships between independent and dependent variables, known as the structural model. In this study, SEM was used to evaluate both the measurement and the structural models. The maximum-likelihood method was employed to determine the direction and strength of correlations between the proposed variables.

## Construct Validation

Confirmatory factor analysis (CFA) was used with IBM SPSS Amos (Version 25) to examine and achieve a significant level of reliability and construct validity for all scales. CFA was used to allow all four constructs to freely co-vary, with each item acting as an indicator for its corresponding latent construct. Furthermore, the maximum-likelihood method was used to estimate the model with the item-correlation matrix as an input. Table 3 depicts the CFA findings, as well as the Cronbach's alphas and composite reliabilities for each construct.

The model fit was evaluated by analyzing the data outputs obtained from validated measurements. The causal relationships between constructs in the structural model were also examined. As indicated in Table 4, the model fit was considered good because all of the model-fit indices fell within the recommended ranges, such as CMIN/DF 2.28 (CMIN = 1,565,  $df$  = 685), RMSEA 0.062, CIF 0.944, NNFI 0.933, and AGFI 0.897 (Alkrajji, 2020; Bentler, 1989; Ghanem et al., 2020; Hair et al., 2019; Hu & Bentler, 1999). Due to the challenges caused by multicollinearity, the findings revealed that the values of the variance inflation factor (VIF) for all constructs were within 1.35–1.82, which is regarded as acceptable.

Table 3. CFA Results

Item	<i>M</i>	Factor Loading	Cronbach's Alpha	Composite Reliability
THSE_1	3.59	0.705	0.85	0.81
THSE_2	3.95	0.73		
THSE_3	4.54	0.751		
THSU_1	4.78	0.746	0.84	0.76
THSU_2	3.89	0.704		
THSU_3	4.58	0.768		
SEF_1	4.77	0.823	0.87	0.85
SEF_2	4.96	0.875		
SEF_3	3.40	0.851		
SEF_4	4.33	0.896		
RECO_1	3.89	0.836	0.81	0.79
RECO_2	4.23	0.777		
RECO_3	4.48	0.795		
RECO_4	3.87	0.885		
FER_1	3.69	0.736	0.91	0.89
FER_2	4.12	0.783		
FER_3	4.54	0.789		
FER_4	4.83	0.732		
FER_5	3.98	0.796		
FER_6	3.57	0.756		
ATTD_1	4.55	0.857	0.85	0.81
ATTD_2	4.67	0.762		
ATTD_3	4.54	0.897		
ATTD_4	3.85	0.758		
BECO_1	3.96	0.805	0.83	0.79
BECO_2	4.56	0.852		
SUNO_1	3.44	0.799	0.95	0.89
SUNO_2	4.35	0.765		
SUNO_3	4.45	0.798		
ORCM_1	4.51	0.814	0.78	0.81
ORCM_2	4.45	0.756		
ORCM_3	4.65	0.789		
ORCM_4	4.38	0.845		

*continued on following page*

Table 3. Continued

Item	<i>M</i>	Factor Loading	Cronbach's Alpha	Composite Reliability
JOSA_1	4.51	0.868	0.82	0.84
JOSA_2	4.20	0.746		
JOSA_3	3.85	0.753		
JOSA_4	3.90	0.768		
ISPM_1	4.78	0.865	0.80	0.77
ISPM_2	4.65	0.785		
ISPM_3	4.96	0.736		
ISPM_4	4.63	0.798		
ISPM_5	4.98	0.742		
ISB_1	3.23	0.701	0.79	0.81
ISB_2	4.47	0.741		
ISB_3	3.23	0.725		
ISB_4	4.41	0.736		
ISB_5	4.74	0.727		

Table 4. Measurement Model Fit Indices

Fit Index	Results	Recommended Value	Reference
CMIN/DF ( $\chi^2/df$ )	1,565/685 = 2.28	$\leq 5$	Hair et al. (2006)
RMSEA	0.062	$\leq 0.08$	Byrne (2001)
CIF	0.944	$\geq 0.90$	Hu & Bentler (1999)
NNFI	0.933	$\geq 0.90$	Hayduk (1987)
AGFI	0.897	$\geq 0.80$	Hayduk (1987)

The convergent validity of the measuring scales was confirmed using three criteria: (1) all indicator loadings must exceed 0.7, (2) construct reliabilities must be higher than 0.8, and (3) the average variance extracted (AVE) for each construct must be significant and larger than its variance, i.e., larger than 0.5 (Fornell & Larcker, 1981). As shown in Table 3, all loadings in this CFA model were above the 0.7 criterion, the composite reliabilities of all constructs ranged between 0.76 and 0.89 and in Table 5 the AVE values ranged between 0.61 and 1.00. As a result, all three convergent validity requirements were met.

Furthermore, the discriminant validity was assessed in accordance with Fornell and Larcker's (1981) recommendation that the square root of the average variance extracted from a specific construct must be greater than the value of the correlation between this construct and others included in the same model. Table 5 shows the list of correlations between all constructs, as well as the square root of the AVE on the diagonal. All AVE values on the diagonal were bigger than the inter-construct correlations. As a result, the assessment of discriminant validity for these constructs was acceptable and verified.

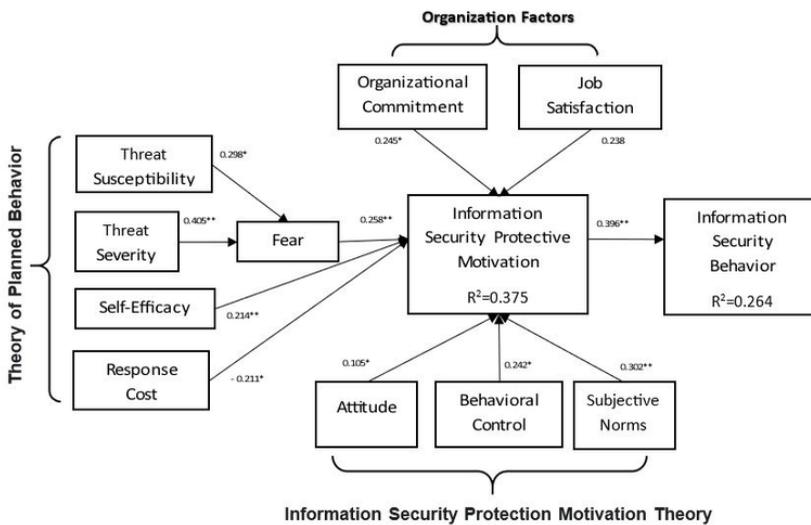
The structural model evaluation results were based on studying the proposed model's predicted capabilities and the relationships between its various constructs, as shown in Fig. 2. The evaluation included scrutinizing collinearity issues, the importance and relevance of path coefficients, and  $R^2$

Table 5. Inter-Item Correlations

	AVE	ATT	BECO	SN	SEF	FA	RC	TSUS	TSEV	OC	JS	PMT	ISPB
ATT	<b>0.67</b>	<b>0.820</b>											
BECO	<b>0.57</b>	0.473	<b>0.754</b>										
SN	<b>0.70</b>	0.355	0.454	<b>0.818</b>									
SEF	<b>0.68</b>	-0.257	0.448	0.489	<b>0.825</b>								
FA	<b>0.63</b>	0.345	0.514	0.446	0.351	<b>0.799</b>							
RC	<b>0.65</b>	0.324	-0.480	-0.444	-0.419	0.382	<b>0.812</b>						
TSUS	<b>0.52</b>	0.485	0.452	0.492	0.561	0.475	-0.367	<b>0.723</b>					
TSEV	<b>0.56</b>	0.256	0.345	0.314	0.506	0.445	-0.225	0.502	<b>0.745</b>				
OC	<b>0.77</b>	0.425	0.395	0.465	0.399	0.485	-0.258	0.365	0.389	<b>0.880</b>			
JS	<b>0.66</b>	0.498	0.369	0.345	0.456	0.452	-0.364	0.452	0.540	0.485	<b>0.815</b>		
PMT	<b>0.62</b>	0.365	0.485	0.413	0.483	0.454	-0.436	0.435	0.410	0.411	0.445	<b>0.789</b>	
ISPB	<b>0.52</b>	0.441	0.352	0.452	0.385	0.426	-0.231	0.360	0.451	0.389	0.487	0.396	<b>0.719</b>

Note. ATT stands for attitude, PBC for perceived behavior control, SN for subjective norms, SE for self-efficacy, FA for fear, RC for response cost, TSUS for threat susceptibility, TSEV for threat severity, OC for organizational commitment, JS for job satisfaction, PMT for protection-motivation theory, and ISPB for information-security protection behavior.

Figure 2. Structural Model



values to describe the degree of variance in a construct. The VIF values were examined to avoid collinearity concerns. If the VIF score was greater than 5.00, there would be collinearity issues and some indicators would need to be removed. According to the findings, the VIF values in this model were less than 5.00 for all predictors, showing no issues with collinearity.

## RESULTS

The evaluation of the structural model was based on the analysis of its predicted capabilities and the relationships between its various constructs, as shown in Fig. 2.

Table 6. Hypothesis Testing

Hypothesis	Estimate	<i>t</i>	Result
H <sub>1</sub> : THSU → FER	0.298*	5.658	Supported
H <sub>2</sub> : THSE → FER	0.405**	11.025	Supported
H <sub>3</sub> : SEF → ISPM	0.214**	3.537	Supported
H <sub>4</sub> : RECO → ISPM	-0.211*	-3.412	Supported
H <sub>5</sub> : FER → ISPM	0.258**	7.524	Supported
H <sub>6</sub> : ATTD → ISPM	0.105*	2.362	Supported
H <sub>7</sub> : BECO → ISPM	0.242*	4.658	Supported
H <sub>8</sub> : SUNO → ISPM	0.302**	3.585	Supported
H <sub>9</sub> : ORCM → ISPM	0.245*	4.852	Supported
H <sub>10</sub> : JOA → ISPM	0.238	2.334	Not Supported
H <sub>11</sub> : ISPM → ISB	0.396**	5.352	Supported

Note. \* =  $p < .05$ , \*\* =  $p < .01$ .

Furthermore, the  $R^2$  values for latent variables were tested. Weak, moderate, and substantial  $R^2$  values are 0.25, 0.50, and 0.75, respectively (Hair et al., 2021). The  $R^2$  was 0.375 for information-security protection motivation and 0.264 for information-security behavior. These values are considered moderate (see Hair et al., 2021). All hypotheses were tested, and relationships between variables are depicted in Fig. 2 and Table 6.

All hypotheses were supported and statistically significant except Hypothesis 10, regarding the relationship between job satisfaction (one of the organizational factors) and information-security protection motivation. First, for the antecedents of protection-motivation theory, the threat-appraisal factors represented in threat susceptibility and threat severity were found to have a significant impact on fear. As presented in Table 6, the first hypothesis was supported, as threat susceptibility of information security had a positive impact on fear ( $\beta = 0.298, p < .05$ ). Threat severity was also found to have a significant impact on fear from information-security risks, supporting the second hypothesis ( $\beta = 0.405, p < .01$ ).

The coping appraisal factors represented in self-efficacy and response cost showed a direct impact on information-security protection motivation, supporting Hypothesis 3 ( $\beta = 0.214, p < .01$ ). Response cost had a negative impact on information-security protection motivation, supporting Hypothesis 4 ( $\beta = -0.211, p < .05$ ), meaning the motivation to protect the security of information was greatly affected by the increase in response costs. While threat-appraisal factors had an impact on fear, fear had a mediating effect between threat susceptibility and threat severity on one hand and information-security protection motivation on the other, supporting Hypothesis 5 ( $\beta = 0.214, p < .01$ ).

With regard to the theory of planned-behavior factors, the findings showed a positive influence on information-security protection motivation from attitude, supporting Hypothesis 6 ( $\beta = 0.105, p < .05$ ); behavioral control, supporting Hypothesis 7 ( $\beta = 0.242, p < .05$ ); and subjective norms, supporting Hypothesis 8 ( $\beta = 0.302, p < .01$ ).

In regard to the organizational factors, organizational commitment had a direct impact on information-security protection motivation, supporting Hypothesis 9 ( $\beta = 0.245, p < .05$ ). In contrast, job satisfaction showed no impact, meaning Hypothesis 10 was not supported ( $\beta = 0.238, p > .05$ ). Finally, there was a significant relationship between information-security protection motivation and information-security behavior, supporting Hypothesis 11 ( $\beta = 0.396, p < .01$ ).

## DISCUSSION AND CONCLUSION

This study explored information-security behavior among information-security professionals in Saudi information-technology companies. The findings offer insights into factors influencing security behavior and contribute to the field as a whole. Factors from protection-motivation theory and the theory of planned behavior along with organizational factors were shown to affect respondent behavior.

Threat appraisal and coping appraisal from protection-motivation theory were essential components of this study. Fear emerged as a significant factor motivating information-security experts to practice coping behaviors, supporting prior research (e.g., Boss et al., 2015; Yang et al., 2020). Information-security experts know, more than other employees, the serious consequences of security risks for the organization. However, Haag et al. (2021) found that 77.6% of information-security research using protection-motivation theory did not recognize fear as a main factor driving behavior. In this study, fear acted as a moderator between threat susceptibility and severity and information-security protection motivation. Thus, inducing fear in information-security professionals can increase their willingness to perform protective behaviors.

Moreover, the coping-appraisal factors (i.e., self-efficacy and response cost) were significant in driving motivation and behavior, supporting similar studies (e.g., Farooq et al., 2019; Haag et al., 2021; Lee & Seomun, 2021; Marshall et al., 2022). The Saudi information-security professionals perceived response cost effectively and reported doing their best to weigh the costs and benefits of a security-protection behavior to safeguard information assets. In addition, self-efficacy gave these professionals the incentive to engage in a behavior that could ensure information security.

Respondents' motivation and actual behavior were tested using the theory of planned behavior. All three factors (attitude, behavioral control, and subjective norms) showed a significant positive effect on motivation and subsequent behavior, agreeing with previous research (e.g., Fishbein & Ajzen, 1975; Lin & Luo, 2021; Venkatesh et al., 2003; Zhang et al., 2020), although other studies (e.g., Rajab & Eydgahi, 2019) revealed no such effect.

Of the two work-related organizational factors (organizational commitment and job satisfaction) tested in the study, only organizational commitment showed a positive effect on information-security protection motivation. Organizational commitment reflects how employees are involved in their organization and like to be related to it. In a study on health-care workers, it was found that commitment could be enhanced through applying effective leadership, implementing satisfaction strategies, and empowering workers (Fantahun et al., 2023). Organizational commitment appeared to raise the morale and involvement in an organization, making information-security professionals more prone to protect organizational assets. In contrast, job satisfaction showed no impact on behavior, suggesting that organization leaders should focus more on linking information-security protection to job satisfaction. This can be achieved by improving the work environment and removing barriers to good behavior.

The factors assessed in this study could help organizations improve the security-protection behavior of information-security professionals by providing adequate training and opportunities for skill development. Organizational leaders and security professionals should work together to solve problems and replace misconceptions with sound practices and procedures (Reznikov, 2023). Positive interaction with these professionals creates a sense of commitment and responsibility to protect their organization. The outcomes of this study showed the effectiveness of understanding threat and coping appraisals.

This study was limited to some of the information-technology companies in Saudi Arabia. Generalizing the outcomes of this study to companies from different parts of the world might not be verified. The study depended on the availability of participants through convenience and snowball sampling; other sampling techniques can be used in future research. The impact of the demographic data of participants on their security behavior was not assessed in this study. Moreover, the survey contained questions that involved some of the behaviors of the information-security professionals, and their honesty in answering these questions might be a matter of concern.

The findings could be extended in future research beyond Saudi Arabia and information-technology organizations. The behavior of information-security professionals could be assessed on the basis of gender, age, job responsibilities, and years of experience. Future research could investigate how well organizational leaders interact and communicate with these professionals to discuss security problems and find solutions. Moreover, other theories could be examined that could explain their security behavior.

## **ACKNOWLEDGMENT**

This research was funded by the Researchers Supporting Project Number RSP2024R453, King Saud University, Riyadh, Saudi Arabia.

## **CONFLICTS OF INTEREST**

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

## **PROCESS DATES**

Received: February 12, 2024, Revision: April 28, 2024, Accepted: April 21, 2024

## **CORRESPONDING AUTHOR**

Correspondence should be addressed to Abdullah Almuqrin (Saudi Arabia, aalmogren@ksu.edu.sa)

## REFERENCES

- Ajmi, L. Hadeel, Alqahtani, N., Ur Rahman, A., & Mahmud, M. (2019). A novel cybersecurity framework for countermeasure of SME's in Saudi Arabia. In *2019 2nd International Conference on Computer Applications & Information Security* (pp. 1–9). IEEE. doi:10.1109/CAIS.2019.8769470
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. doi:10.1002/hbe2.195
- Al-Qirim, N., Rouibah, K., Abbas, H., & Hwang, Y. (2022). Factors affecting the success of social commerce in Kuwaiti microbusinesses: A qualitative study. [JGIM]. *Journal of Global Information Management*, *30*(1), 1–31. doi:10.4018/JGIM.313944
- Alaidaros, H., & Albeedh, S. (2022). Towards studying the relationship between job satisfaction and organizations' information security. In *2022 International Conference on Intelligent Technology, System and Service for Internet of Everything* (pp. 1–6). IEEE. doi:10.1109/ITSS-IoE56359.2022.9990932
- AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Government Information Quarterly*, *39*(4), 101721. doi:10.1016/j.giq.2022.101721
- Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences (Basel, Switzerland)*, *11*(8), 3383. doi:10.3390/app11083383
- Alkrajji, A. I. (2020). Citizen satisfaction with mandatory e-government services: A conceptual framework and an empirical validation. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 117253–117265. doi:10.1109/ACCESS.2020.3004541
- Almuqrin, A., Mutambik, I., Alomran, A., & Zhang, J. Z. (2023a). Enforcing information system security: Policies and procedures for employee compliance. [IJSWIS]. *International Journal on Semantic Web and Information Systems*, *19*(1), 1–17. doi:10.4018/IJSWIS.331396
- Almuqrin, A., Mutambik, I., Alomran, A., & Zhang, J. Z. (2023b). Information system success for organizational sustainability: Exploring the public institutions in Saudi Arabia. *Sustainability (Basel)*, *15*(12), 9233. doi:10.3390/su15129233
- Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. doi:10.1037/0033-2909.103.3.411
- Ataei Nezhad, M., Barati, H., & Barati, A. (2022). An authentication-based secure data aggregation method in internet of things. *Journal of Grid Computing*, *20*(3), 29. doi:10.1007/s10723-022-09619-w PMID:35991685
- Avraam, D., Jones, E., & Burton, P. (2022). A deterministic approach for protecting privacy in sensitive personal data. *BMC Medical Informatics and Decision Making*, *22*(1), 24. doi:10.1186/s12911-022-01754-4 PMID:35090447
- Baroudi, S., Tamim, R., & Hojeij, Z. (2022). A quantitative investigation of intrinsic and extrinsic factors influencing teachers' job satisfaction in Lebanon. *Leadership and Policy in Schools*, *21*(2), 127–146. doi:10.1080/15700763.2020.1734210
- Bascomb, J. (2020). *Qualitative case study exploring the factors to improve employee satisfaction and the organizational citizenship behavior of cybersecurity professionals in the Department of Defense* [Doctoral dissertation, Northcentral University]. <https://www.proquest.com/openview/34da6ee370152f6be6183c024bef336e/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Bentler, P. M. (1989). *EQS structural equations program manual*. BMDP Statistical Software.
- Bolek, V., Romanová, A., & Korček, F. (2023). The information security management systems in e-business. [JGIM]. *Journal of Global Information Management*, *31*(1), 1–29. doi:10.4018/JGIM.316833

- Bos, J. (2020). *Research ethics for students in the social sciences*. Springer., doi:10.1007/978-3-030-48415-6
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Management Information Systems Quarterly*, 39(4), 837–864. doi:10.25300/MISQ/2015/39.4.5
- Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing*, 1(1), 55–86. doi:10.1207/S15327574IJT0101\_4
- Cai, Y., Zhang, X., Niu, H., Li, W., Huo, D., He, J., & Chen, H. (2023). Privacy and information disclosure: Dynamic digital governance in response to COVID-19. [JGIM]. *Journal of Global Information Management*, 31(6), 1–22. doi:10.4018/JGIM.321182
- Chang, A. J., Wu, C., & Liu, H. (2012). The effects of job satisfaction and organization commitment on information security policy adoption and compliance. In *Proceedings of the IEEE International Conference on Management of Innovation & Technology* (pp. 442–446). IEEE. doi:10.1109/ICMIT.2012.6225846
- Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, 55(8), 1049–1060. doi:10.1016/j.im.2018.05.011
- Ennida, K., & Allouani, S. A. (2023). Job satisfaction and organizational commitment of teacher-researchers through organizational citizenship behavior: A literature review. *Open Journal of Social Sciences*, 11(3), 164–184. doi:10.4236/jss.2023.113011
- Ezati Rad, R., Mohseni, S., Kamalzadeh Takhti, H., Hassani Azad, M., Shahabi, N., Aghamolaei, T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: A cross-sectional study. *BMC Public Health*, 21(1), 466. doi:10.1186/s12889-021-10500-w PMID:33685426
- Fantahun, B., Dellie, E., Worku, N., & Debie, A. (2023). Organizational commitment and associated factors among health professionals working in public hospitals of southwestern Oromia, Ethiopia. *BMC Health Services Research*, 23(1), 180. doi:10.1186/s12913-023-09167-3 PMID:36810031
- Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019). *Factors affecting security behavior of Kenyan students: An integration of protection motivation theory and theory of planned behavior*. In *2019 IEEE AFRICON*. IEEE., doi:10.1109/AFRICON46755.2019.9133764
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research*, 18(1), 39–50. doi:10.1177/002224378101800104
- Gaurav, A., & Panigrahi, P. K. (2022). Analysis of security paradigms for resource and infrastructure management in global organizations. [JGIM]. *Journal of Global Information Management*, 31(2), 1–11. doi:10.4018/jgim.320528
- Ghanem, M., Elshaer, I., & Shaker, A. (2020). The successful adoption of IS in the tourism public sector: The mediating effect of employees' trust. *Sustainability (Basel)*, 12(9), 3877. doi:10.3390/su12093877
- GlobalData. (2023, December 30). *Saudi Arabia ICT market report*. Retrieved from <https://www.globaldata.com///arabia-ict-market-analysis>
- Guzmán, S. A., Fóster, P. F., Ramírez-Correa, P., Grandón, E. E., & Alfaro-Perez, J. (2018). Information systems and their effect on organizational performance: An inquiry into job satisfaction and commitment in higher education institutions. *Journal of Information Systems Engineering & Management*, 3(4), 26–31. doi:10.20897/jisem/3937

- Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *The Data Base for Advances in Information Systems*, 52(2), 25–67. doi:10.1145/3462766.3462770
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (6th ed.). Pearson.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R*. Springer. doi:10.1007/978-3-030-80519-7
- Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2–16. doi:10.1080/10580530.2015.117842
- Hayduk, L. A. (1987). *Structural equation modeling with LISREL: Essentials and advances*. Johns Hopkins University Press.
- Hsu, W. C., & Lee, M. H. (2023). Semantic technology and anthropomorphism: Exploring the impacts of voice assistant personality on user trust, perceived risk, and attitude. *Journal of Global Information Management*, 31(1), 1–21. doi:10.4018/JGIM.318661
- Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1–55. doi:10.1080/10705519909540118
- Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's internet of things. *Heliyon*, 7(3), e06522. doi:10.1016/j.heliyon.2021.e06522 PMID:33768182
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. doi:10.1016/j.cose.2011.10.007
- Irwin, L. (2022, August 12). *5 real-life examples of data breaches caused by insider threats*. Retrieved from <https://www.grcilaw.com/blog/5-real-life-examples-of-data-breaches-caused-by-insider-threats>
- Jayawardena, N. S., Chavali, K., Dewasiri, N. J., Perera, C. H., Koswatte, I., Pereira, V., Gupta, M., & Mardani, A. (2023). Exploring the challenges in developing and managing digital agility among Sri Lankan family business owners during the economic crisis situation. [JGIM]. *Journal of Global Information Management*, 31(8), 1–22. doi:10.4018/JGIM.326763
- Kim, J., Yang, K., Min, J., & White, B. (2022). Hope, fear, and consumer behavioral change amid COVID-19: Application of protection motivation theory. *International Journal of Consumer Studies*, 46(2), 558–574. doi:10.1111/ijcs.12700 PMID:34220343
- Kumar, A., Shankar, A., Behl, A., Gupta, B. B., & Mavuri, S. (2023). Lights, camera, metaverse! Eliciting intention to use industrial metaverse, organizational agility, and firm performance. [JGIM]. *Journal of Global Information Management*, 31(8), 1–20. doi:10.4018/JGIM.333169
- Lee, E., & Seomun, G. (2021). Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *International Journal of Environmental Research and Public Health*, 18(4), 2084. doi:10.3390/ijerph18042084 PMID:33669926
- Li, C., Feng, W. X., Han, S., Gupta, S., & Kamble, S. (2022). Digital adaptive governance, digital transformation, and service quality in logistics enterprises. [JGIM]. *Journal of Global Information Management*, 30(1), 1–26. doi:10.4018/JGIM.309377
- Liang, X., Ruan, W., Xu, Z., & Liu, J. (2022). Analysis of safe storage of network information data and financial risks under blockchain combined with edge computing. [JGIM]. *Journal of Global Information Management*, 30(11), 1–20. doi:10.4018/JGIM.312580

- Lin, B., & Zhu, R. (2023). What information do we have on the government's environmental management? A perspective of energy and carbon performance in China's mining industry. [JGIM]. *Journal of Global Information Management*, 31(1), 1–22. doi:10.4018/JGIM.333237
- Lin, C., & Luo, X. (2021). Toward a unified view of dynamic information security behaviors: Insights from organizational culture and sensemaking. *The Data Base for Advances in Information Systems*, 52(1), 65–90. doi:10.1145/3447934.3447940
- Liu, C., Liang, H., Wang, N., & Xue, Y. (2022). Ensuring employees' information security policy compliance by carrot and stick: The moderating roles of organizational commitment and gender. *Information Technology & People*, 35(2), 802–834. doi:10.1108/ITP-09-2019-0452
- Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54, 102152. doi:10.1016/j.ijinfomgt.2020.102152
- Locke, E. (1976). The nature and causes of job satisfaction. In M. D. Dunnette (Ed.), *The handbook of industrial and organizational psychology* (pp. 1297–1349). John Wiley & Sons.
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. doi:10.1016/0022-1031(83)90023-9
- Malik, H. A. M., Shah, A. A., Muhammad, A. H., Kananah, A., & Aslam, A. (2022). Resolving security issues in the IoT using blockchain. *Electronics (Basel)*, 11(23), 3950. doi:10.3390/electronics11233950
- Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. In S. Papagiannidis (Ed.), *TheoryHub book*. Retrieved from <https://open.ncl.ac.uk/theory-library/protection-motivation-theory.pdf>
- Marshall, B., Curry, M., Crossler, R. E., & Correia, J. (2022). Machine learning and survey-based predictors of infosec non-compliance. *ACM Transactions on Management Information Systems*, 13(2), 1–20. doi:10.1145/3466689
- Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, 75, 147–166. doi:10.1016/j.cose.2018.01.020
- Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, 1(1), 61–89. doi:10.1016/1053-4822(91)90011-Z
- Meyer, J. P., & Allen, N. J. (1997). Commitment in the workplace: Theory, research, and application. *Sage (Atlanta, Ga.)*. Advance online publication. doi:10.4135/9781452231556
- Meyer, J. P., Allen, N. J., & Smith, C. A. (1993). Commitment to organizations and occupations: Extension and test of a three-component conceptualization. *The Journal of Applied Psychology*, 78(4), 538–551. doi:10.1037/0021-9010.78.4.538
- Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106–143. doi:10.1111/j.1559-1816.2000.tb02308.x
- Mutambik, I., Almuqrin, A., Alharbi, F., & Abusharhah, M. (2023a). How to encourage public engagement in smart city development—Learning from Saudi Arabia. *Land (Basel)*, 12(10), 1851. doi:10.3390/land12101851
- Mutambik, I., Lee, J., Almuqrin, A., Alkhanifer, A., & Baihan, M. (2023c). Gulf Cooperation Council countries and urbanisation: Are open government data portals helping? *Sustainability (Basel)*, 15(17), 12823. doi:10.3390/su151712823
- Mutambik, I., Lee, J., Almuqrin, A., & Zhang, J. Z. (2023b). Transitioning to smart cities in Gulf Cooperation Council countries: The role of leadership and organisational culture. *Sustainability (Basel)*, 15(13), 10490. doi:10.3390/su151310490
- Mutambik, I., Lee, J., Almuqrin, A., Zhang, J. Z., Baihan, M., & Alkhanifer, A. (2023d). Privacy concerns in social commerce: The impact of gender. *Sustainability (Basel)*, 15(17), 12771. doi:10.3390/su151712771

- Oakley, M., Mohun Himmelweit, S., Leinster, P., & Casado, M. R. (2020). Protection motivation theory: A proposed theoretical extension and moving beyond rationality—the case of flooding. *Water (Basel)*, *12*(7), 1848. doi:10.3390/w12071848
- Oz, E. (2001). Organizational commitment and ethical behavior: An empirical study of information system professionals. *Journal of Business Ethics*, *34*(2), 137–142. doi:10.1023/A:1012214017119
- Pearson, D. L. (2021). *Chaotic and unexplored: The complex relationship between security professionals, data breaches, and malicious actors* [Doctoral dissertation, University of Fairfax]. ProQuest. <https://www.proquest.com/docview/2551520225>
- 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. doi:10.1080/07421222.2015.1138374
- Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. *Applied Sciences (Basel, Switzerland)*, *12*(3), 1598. doi:10.3390/app12031598
- Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223. doi:10.1016/j.cose.2018.09.016
- Reznikov, D. (2023, January 11). *How to improve communication between information security staff and management*. Kaspersky. Retrieved from <https://www.kaspersky.com/blog/business-soc-communications/46753/>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803 PMID:28136248
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). Guildford Press.
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors (Basel)*, *23*(15), 6666. doi:10.3390/s23156666 PMID:37571451
- Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. doi:10.1016/j.chb.2015.12.037
- Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, *59*(4), 344–353. doi:10.1080/08874417.2017.1368421
- Spector, P. E. (1985). Measurement of human service staff satisfaction: Development of the Job Satisfaction Survey. *American Journal of Community Psychology*, *13*(6), 693–713. doi:10.1007/BF00929796 PMID:4083275
- Taheri-Kharameh, Z., Bashirian, S., Heidarimoghdam, R., Poorolajal, J., Barati, M., & Rásky, É. (2020). Predictors of fall protective behaviors among Iranian community-dwelling older adults: An application of the protection motivation theory. *Clinical Interventions in Aging*, *15*, 123–129. doi:10.2147/CIA.S224224 PMID:32103913
- Tan, K. L., Sia, J. K., & Tang, K. H. D. (2022). Examining students' behavior towards campus security preparedness exercise: The role of perceived risk within the theory of planned behavior. *Current Psychology (New Brunswick, N.J.)*, *41*(7), 4358–4367. doi:10.1007/s12144-020-00951-6
- 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. doi:10.1016/j.giq.2021.101572 PMID:35719729
- Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, *48*(8), 1565–1585. doi:10.1108/K-05-2018-0226
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. doi:10.1287/mnsc.46.2.186.11926

- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, 27(3), 425–478. doi:10.2307/30036540
- Wall, J. D., Palvia, P., & D'Arcy, J. (2022). Theorizing the behavioral effects of control complementarity in security control portfolios. *Information Systems Frontiers*, 24(2), 637–658. doi:10.1007/s10796-021-10113-z
- Wang, Y., Xue, W., & Zhang, A. (2023). Application of big data technology in enterprise information security management and risk assessment. [JGIM]. *Journal of Global Information Management*, 31(3), 1–16. doi:10.4018/JGIM.324465
- Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information and Computer Security*, 28(5), 743–761. doi:10.1108/ICS-08-2019-0095
- Yang, M., & Xu, P. (2021). Understanding the antecedents of knowledge sharing behavior from the theory of planned behavior model: Cross-cultural comparisons between mainland China and Malaysia. *Frontiers in Psychology*, 12, 772764. doi:10.3389/fpsyg.2021.772764 PMID:34867681
- Yang, N., Singh, T., & Johnston, A. (2020). A replication study of user motivation in protecting information security using protection motivation theory and self-determination theory. *AIS Transactions on Replication Research*, 6, 10.
- Yeng, P. K., Wolthusen, S. D., & Bian, Y. (2021). Adopting vulnerability principle as the panacea for security policy monitoring. [IJACSA]. *International Journal of Advanced Computer Science and Applications*, 12(3). Advance online publication. doi:10.14569/IJACSA.2021.0120303
- Zhang, X., Liu, S., Wang, L., Zhang, Y., & Wang, J. (2020). Mobile health service adoption in China: Integration of theory of planned behavior, protection motivation theory and personal health differences. *Online Information Review*, 44(1), 1–23. Advance online publication. doi:10.1108/OIR-11-2016-0339
- Zhen, J., Xie, Z., & Dong, K. (2020). Relationship between information security behavior and satisfaction degree of psychological needs and the mediation effect of team effectiveness and organizational commitment. *Revista Argentina de Clínica Psicológica*, 29(1), 442. doi:10.24205/03276716.2020.60

*Abdullah Almuqrin is working as an associate professor at King Saud University, Information Science Department. He was interested in computers which motivated him after he completed his high school to join the computer science program at King Saud University (KSU) in Saudi Arabia. Then, he completed his master's degree majored in information systems from Lawrence Technological University (USA). Finally, he completed his PhD in information Assurance from Eastern Michigan University (USA). Research interest: Information systems, knowledge management, knowledge sharing, innovation technologies, Social media (networks), and privacy and information security.*

*Ibrahim Mutambik is an Associate Professor in the Department of Information Science at King Saud University in Saudi Arabia, where he also holds the prestigious position of Head of Data Management Office at King Saud University and the University's Medical City. Dr. Mutambik' embarked on his academic journey at Jazan University, where he secured his Bachelor's degree in Computer Science. His thirst for knowledge led him to Heriot-Watt University, UK, where he earned his Master's degree from the Department of Computer Science. Dr. Mutambik further pursued his passion for the field at the University of Edinburgh, UK, earning his PhD from the esteemed Informatics School. His academic pedigree is complemented by an array of research publications in Scopus and Web of Science-indexed journals, marking him as a thought leader in the realm of informatics.*

*Justin Zhang is a faculty member in the Department of Management at Coggin College of Business in University of North Florida. He received his Ph.D. in Business Administration with a concentration on Management Science and Information Systems from Pennsylvania State University, University Park. His research interests include economics of information systems, knowledge management, electronic business, business process management, information security, and social networking. He has published research articles in various scholarly journals, books, and conference proceedings. He is the editor-in-chief of the Journal of Global Information Management. He also serves as an associate editor and an editorial board member for several other journals.*

*Hashem Farahat S. Academic and Professional Experiences: 2010-Present: Professor, Department of Information Science, King Saud University; coordinator of Program of Graduate Studies, member of Editorial Board; Journal of " Information Studies" issued by Saudi Association for Libraries and Information and, Member of Editorial Board; " Cybrarian" an electronic Scholarly peer reviewed Journal for Library and Information Science Studies; and member and reviewer, many Scientific Journals and Committees. Publications: published about 16 books and 58 scientific papers in refereed journals and conferences in many research areas of interest: Bibliometric, Scientometrics and all related areas, Research Methods in Information Studies and Social Sciences, Knowledge Management, Research Data Management, Information Storage and Retrieval, and Metadata and Organization of Information. Accounts in Scientific Networks: Google Scholar (<https://scholar.google.com/citations?hl=en&user=cMzjVAAAAAJ>), ORCID (<https://orcid.org/my-orcid?orcid=0000-0002-8539-3581>), Web of Science ResearcherID (ABF-5660-2021 <https://www.webofscience.com/wos/author/record/2434151>), and Researchgate ([https://www.researchgate.net/profile/Hashem\\_Farahat](https://www.researchgate.net/profile/Hashem_Farahat))*

*Zahyah H. Alharbi received her M.Sc. in Management Information Systems from Northern Illinois University, IL, USA, and her Ph.D. in Computing Sciences with a focus on data mining from the University of East Anglia, Norwich, UK, in 2019. She is an esteemed Assistant Professor in the Department of Management Information Systems at King Saud University, renowned for her extensive contributions to ISI journals. Her expertise spans machine learning, data privacy, analytics, social media analysis, information security, and the establishment of robust data governance frameworks.*