Article

Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector

Sultan T. Alanazi 1,*, Mohammed Anbar 1,†, Shouki A. Ebad 2 □ and Shankar Karuppayah 1 and Hadeer A. Al-Ani 3

1 National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang 11800 USM, Malaysia; Shankar@nav6.usm.my
2 Computer Science Department, Faculty of Science, Northern Border University, Arar 73222, Saudi Arabia; Shouki.abbad@nbu.edu.sa
3 Department of Public Health, School of Medicine, University of California Davis, Davis, CA 95616, USA; Haalani@ucdavis.edu
* Correspondence: sultan@nav6.usm.my (S.T.A.); anbar@nav6.usm.my (M.A.)

Received: 25 August 2020; Accepted: 15 September 2020; Published: 18 September 2020

Abstract: The adoption of health information systems provides many potential healthcare benefits. The government of the Kingdom of Saudi Arabia has subsidized this field. However, like those of other less developed countries, organizations in the Kingdom of Saudi Arabia struggle to secure their health information systems. This issue may stem from a lack of awareness regarding information security. To date, most related studies have not considered all of the factors affecting information security compliance behavior (ISCB), which include psychological traits, cultural and religious beliefs, and legal concerns. This paper aims to investigate the usefulness of a theory-based model and determine the predictors of ISCB among healthcare workers at government hospitals in the Kingdom of Saudi Arabia. The study investigated 433 health workers in Arar, the capital of the Northern Borders Province in the Kingdom of Saudi Arabia. Two phases involved in this study were the hypothetical model formulation and identification of ISCB predictors. The results suggest that moderating and non-common factors (e.g., religion and morality) impact ISCB, while demographic characteristics (e.g., age, marital status, and work experience) do not. All published instruments and theories were embedded to determine the most acceptable theories for Saudi culture. The theory-based model of ISCB establishes the main domains of theory for this study, which were religion/morality, self-efficacy, legal/punishment, personality traits, cost of compliance/noncompliance, subjective norms, information security policy, general information security, and technology awareness. Predictors of ISCB indicate that general information security, followed by self-efficacy and religion/morality, is the most influential factor on ISCB among healthcare workers in the Kingdom of Saudi Arabia. This study is considered as the first to present the symmetry between theory and actual descriptive results, which were not investigated before.

Keywords: behavioral theory; health information system; information security; information security compliance behavior

1. Introduction

The adoption of health information systems (HISs) provides many potential benefits, such as improved quality of care, the reduction of medical errors, and enhanced access to information [1,2]. A reliable and coherent information system (IS) requires a solid security framework that follows the CIA triad (i.e., confidentiality, integrity, and availability). Moreover, employee behavior is a
significant factor in maintaining information security and information policy compliance. However, this factor is not easily controlled [3]. Hwang et al. claimed that insider threats result from misuse actions, including authority abuse, unawareness of policy, technical issues with software and hardware, and information mishandling [4]. In general, insider threats may be more dangerous than outsider threats because employees have prior information about their organization’s security policies and can access it’s IS [2,5–7]. For this reason, organizations normally establish IS policies to enhance employee awareness, which is the cornerstone of information security compliance behavior (ISCB).

To keep pace with developed countries in the field of healthcare, the government of the Kingdom of Saudi Arabia (KSA) has subsidized this field. However, issues have occurred relating to protecting patient privacy and preventing data leaks or tampering by healthcare employees, including physicians and nurses [2,7]. This study aims to develop a model based on a specific theory of ISCB in order to minimize such issues. The rest of the paper is structured as follows: Section 2 describes the problem statement and the study’s contribution. Section 3 provides a brief background on existing behavioral theories. The pertinent literature is reviewed in Section 4, before Section 5 outlines the research methodology. Section 6 presents a hypothetical ISCB model and its related variables. Section 7 discusses the proposed model and findings, before Section 8 outlines the relevant conclusions and proposes future research directions on this topic.

2. Problem Statement and Study’s Contribution

The KSA has pointed out weaknesses in the country’s management of healthcare systems attributed to a series of obstacles and influencing factors, such as a lack of awareness or an adverse environment [8,9]. Moreover, studies conducted to date (especially those conducted in Middle Eastern countries such as the KSA) have suffered from weak study designs and academic research procedures [10,11] and/or have covered only common factors affecting ISCB. In other words, the majority of studies cover only the relevant factors of their research problems and have neglected other factors affecting information security behavior, such as environmental, social, and psychological factors of the community aspects [12,13]. This presents a difficulty in considering all factors of information security behavior, due to the existence of several theories and domains. Lebek et al., in [14], conducted a theory-based literature review of employee ISCB theories found in 113 studies. They identified several research gaps for 54 theories of security behavior, due to: the inability to generalize study outcomes, failure to involve all personal and environmental factors for each study and community, and non-matched beliefs between the theories and actual practice. Therefore, most of the studies conducted both internationally and locally (i.e., in Arab countries and the KSA) failed to cover all of the factors affecting security behavior. For example, psychological factors have been proven to be relevant [9], but they have not been studied in the KSA. Furthermore, variables such as personality traits, religion/morality, and legal consequences/punishment are believed to moderate ISCB. The main contribution of this study is its insight into the influence of such factors among healthcare employees of the KSA.

3. Background on Theories of Information Security Compliance Behavior

While there are many theories pertaining to information security behavior, the following subsections highlight those specifically related to this study.

3.1. Theory of Planned Behavior

This expectancy-value theory is used to predict behavioral intentions that in turn lead to actual behaviors and is applied in multiple research areas [15]. The theory of planned behavior (TPB) considers three main factors affecting individuals’ behavior: their own attitude towards a given action, their perception of others’ appraisal of said action (subjective norms), and their perceived ability to carry it out (perceived behavioral control) [16]. Attitude, as an essential factor of this theory, explains the activities of social psychology according to several studies. According to the TPB,
individuals will engage in a given behavior only if their attitude, subjective norms, and perceived behavioral control are all positive in relation to the behavior [17].

3.2. General Deterrence Theory/Neutralization Theory

In the field of criminology, Reference [18] predicted criminal behavior based on deterrence and fear beliefs. They observed that severe punishments and sanctions reduce criminal intentions, which in turn prevent criminal action. This theory is implemented by the organization as part of their policy to increase awareness of information security system violations.

3.3. Protection Motivation Theory

This theory posits that human protective behavior is based on three processes: cognitive appraisal, threat appraisal, and coping response appraisal. Threat appraisal refers to individuals’ beliefs about the severity of a given threat and their perceived vulnerability to such a threat. Coping appraisal concerns individuals’ beliefs about response efficacy, that is, the effectiveness of actions recommended to avoid or reduce the threat in question, and self-efficacy, i.e., their own ability to execute the recommended actions. The protection motivation theory (PMT) may be applied to ISCB studies [16,17]. In the realm of information security behavior in particular, it has been expanded to include factors such as technology awareness and social aspects [19].

3.4. Diffusion of Innovation/Technology Awareness Theory

The technology acceptance model (TAM) models users’ acceptance of a given technology, based mainly on two factors: perceived usefulness and perceived ease-of-use. Perceived usefulness refers to the technology’s ability to enhance users’ performance. Perceived ease-of-use refers to the extent to which users believe that the technology will require little effort, which is an essential factor when it comes to employee behavior in a technologically developed era [16,20]. The TAM was reformulated by [19] for adaptation to several fields, such as politics, public health, communications, history, economics, and education. Diffusion of innovation (DOI) is a new theory explaining how users’ heightened awareness of a given technology affects their decision to adopt it. More specifically, there are four factors affecting adoption: the innovative technology itself, the communication channel through which it spreads, the time it takes to do so, and the social system it caters to.

3.5. Rational Choice Theory

Bulgurcu et al. [5] adapted this theory to focus on employees’ compliance with their organization’s information security policies. According to this theory, employees’ decisions regarding compliance are based on their evaluation of its costs and benefits. Few studies are closely related to the present research in their examination of ISCB. However, to the best of the authors’ knowledge, no study has explored ISCB in the KSA. This paper aims to fill that gap.

3.6. Cognitive Moral Development Theory

This theory refers to the respect of principles to determine the actions required for a situation. There are six stages of moral judgment theory; Stages 1 and 2, pre-conventional; Stages 3 and 4, conventional; and Stages 5 and 6, post-conventional. These stages are associated with the social aspects, culture, individual, rules, and laws [21].

The selection of theories considered in this study is based on acceptable models of ISCB mentioned in literature studies. Hamed Taherdoost and Lebek et al. [22] produced a review on the acceptable models of ISCB [22,23]. Table 1 illustrates the common theories used by the majority of studies and outlines the benefits in the selection of theories by this study.
Table 1. Theories and their relationships to information security compliance behavior.

| Theory                                | Relationship to Behavior                                                                 | References                       |
|---------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------|
| Theory of planned behavior            | (1) It is an expectancy-value model. (2) Causes the response of actual behaviors.        | Ajzen, 1991 [15], Ifinedo, 2012 [24]. |
| General deterrence theory (GDT)       | Predicts criminal behaviors based on deterrence and fear beliefs, which in turn significantly affect the motivation and self-aspects of employees. | Gibbs, 2018 [18].                |
| Protection motivation theory          | (1) Determines the behaviors of subjects to avert the consequences induced by violations. (2) Investigates methods to protect behavior based on cognitive appraisal. | Brown, 2017 [25].                |
| Cognitive moral development           | (1) Moral reasoning influences behavior and policy violations. (2) It measures employee adherence to information security policies. | Myyry et al., 2009 [21].         |
| Diffusion of innovation               | (1) Improves the awareness of employees to support their decisions, to increase certainty and minimize uncertainty. (2) Training employees makes their security behavior more satisfactory. | Weigel et al., 2014. [26].       |
| Rational choice theory                | Supports the decisions of individuals based on the principle of cost/benefit.             | Bulgurcu et al., 2010. [5].      |

4. Literature Studies

Li and Hoffman [27] investigated the relationship between employees’ ISCB and punishment severity in a series of organizations. Using the general deterrence theory (GDT), they identified demographic and human reasons behind IS violations and deployed a series of theories (i.e., GDT, PMT, and TPB) to evaluate predictors of ISCB. They found that ISCB was influenced by awareness, sanction certainty, and self-efficacy [28]. They also evaluated the potential factors influencing ISCB and information security awareness in business contexts. These factors included security education, security policies, knowledge of a physical system, security visibility, and management participation. The results indicated that all factors except for the knowledge of a physical system affected information security awareness [4] Furthermore, they used two theories, PMT and GDT, to determine factors related to ISCB. The domains evaluated through the PMT were perceived threat vulnerability, threat severity, response efficacy, and self-efficacy. Factors covered by the GDT included sanction certainty and severity. Self-efficacy was the only significant predictor of ISCB compared to the other variables. Hwang et al. [4] based their model on a series of domains, including employees’ awareness of and satisfaction with information security, their perception of its usefulness, fairness, and quality, self-efficacy, and certain organizational factors. Results showed that awareness, perceived quality, and self-efficacy significantly influenced employees’ ISCB. Ryutov et al. [9] also based their model on a series of domains, including employees’ awareness of and satisfaction with information security, perception of its usefulness, fairness, and quality, self-efficacy, and certain organizational factors. The results also showed that awareness, perceived quality, and self-efficacy significantly influenced employees’ ISCB. Ryutov et al. [9] focused on examining the impact of human factors on ISCB. In particular, they considered behavior deterrence, policy stringency, employee commitment to and awareness of information security systems, management support, information security culture, and demographic characteristics. All factors except for policy stringency and employee commitment were demonstrated to influence security behavior. Bauer and Bernroider [29] used the theory of reasoned action, the knowledge/attitude/behavior model, and the neutralization theory to study several factors in relation to ISCB, namely: attitude, social norms, neutralization techniques, information security awareness, and demographic characteristics. They found that only
the first three significantly affected ISCB. Guhr et al. [30] examined how management leadership style influenced employees’ ISCB. They considered transformational leadership, transactional leadership, and passive/avoidant leadership. The findings showed that transformational leadership was the only significant factor. Humaidi and Balakrishnan [31] used the TPB and other theories to build their model. They considered management support, self-efficacy, perceived trust, and compliance behavior as potentially relevant predictors of ISCB, all of which were found to be significant. Likewise, Rogers [19] relied on TPB to determine the factors influencing ISCB. The findings revealed that behavioral belief, social pressure, and compliance knowledge had a positive and significant impact. Herath and Rao [32] studied attitude, perceived behavioral control, and subjective norms as factors, but only the latter was shown to have an impact on ISCB. AlKalbani et al. [3] implemented institutional theory to examine the impacts of legal punishment, security benefits, social pressure, and management commitment, and all were found to be influential.

5. Research Methodology

A questionnaire-based survey was used to collect responses from participants related to their information security behavior and knowledge. This method is similar to that employed by several existing studies [5,17].

5.1. Objectives

The primary goal of this study is to investigate the usefulness of the proposed model for determining predictors of ISCB among healthcare workers at governmental hospitals in the KSA. The following objectives were pursued to achieve the main goal of this study:

1. to investigate the effect of non-common factors (e.g., religion/morality, personality traits, and legal consequences/punishment) on ISCB among healthcare employees in the KSA;
2. to explore the effect of moderators on ISCB among healthcare employees in the KSA;
3. to examine the impact of demographic characteristics on ISCB among healthcare employees in the KSA;
4. to propose a final, theory-based model of ISCB among healthcare workers in the KSA.

5.2. Population

Participants were drawn from governmental healthcare centers in Arar, the capital of the Northern Border Province in the KSA. A total of 2297 workers from five different hospitals and centers were considered, as shown in Table 2.

| Hospital                        | Number of Healthcare Workers |
|---------------------------------|------------------------------|
| Arar Central Hospital           | 750                          |
| Prince Abdulaziz Bin Musaad Hospital | 466                          |
| Maternity and Children Hospital | 697                          |
| Al-Amal Complex for Mental Health | 248                          |
| Extended Care Facility          | 100                          |
| **Total**                       | **2297**                     |

The only exclusion criterion was having been previously punished or reported for a work-related violation. The study was conducted between November and December 2019.
5.3. Sampling of the Present Study

Study participants were selected using the random sampling technique and were chosen randomly from one pool. They were then invited to enroll in the study using an electronic survey. All participants were involved voluntarily, and signed consent forms were collected from all participants.

5.4. Statistical Analysis

SmartPLS v3 and SPSS Statistics v22 were used for data analysis. The purpose of using SmartPLS software was to develop the theory of ISCB for Saudi employees, while SPSS is a program used to determine predictors, where the predictor with the greatest influence can be observed alongside the other domains. Kim et al. also investigated the effects of security behavior using the multi-theory model. They believed that theory and descriptive analysis was required to approve the performance of this model, i.e., that performance depends on the mix between the theory and actual results [17]. Therefore, the present study developed the model in a pilot study as a first phase and determined the predictors in a second phase. The reasons for using a regression test to predict factors influencing the information compliance behavior were as follows: (1) the assumptions of any statistical test should meet the requirements, which cannot be achieved using the SmartPLS; (2) the SmartPLS determines the influence of each variable separately without taking into account the influence of other variables; (3) the objective of the present study is to identify the predictors having the greatest impact on the ISCB, which could not be measured using the SmartPLS; (4) the regression test and results using SPSS are more robust than results obtained from SmartPLS; and (5) the influence of demographic characteristics, as predictors, showed weaker results with the use of SmartPLS than other software [33]. Results were considered significant when their p-values were lower than 0.05. SmartPLS was used to implement structural equation modeling (SEM), confirmatory factor analysis, and exploratory factor analysis in the first phase. Then, SPSS was used to determine the predictors of ISCB in the second phase. Confirmatory factor analysis was used to determine the impact of independent variables (domains) on the main dependent variable (ISCB) and to approve the construction of the model. Exploratory factor analysis was applied to determine the validity of the study’s instruments. Cronbach’s alpha was used to determine the internal consistency of separate items and overall instruments, while multiple linear regressions were used to determine the predictors of ISCB and the impact of their interactions on ISCB. The dummy method of a regression test was used to determine which variable was more influenced compared to other variables. This type of regression identifies the most significant sub-variables, such as female, single, etc.

5.5. First Phase and Pilot Study

A pilot test was conducted in order to improve the clarity of the survey questions and address critical issues concerning statistical variables. Several steps were performed to approve the validity of questionnaire items. These steps involved panel validity, domain validity, and item validity. For statistical approval, SEM was performed to identify the dimensions and path coefficients of the theory. The number of participants was 100.

5.5.1. Panel Validity

Eight field professionals, academics, and researchers in the KSA evaluated every domain and item considered in the pilot study, as well as their potential influence on ISCB and made recommendations to omit or merge certain items. A Cohen’s kappa test was conducted to determine inter-rater reliability, that is the coefficient of agreement among panelists. Values ranged between 0.89 and 1.00 (the optimal standard value being 0.80). The total number of factors involved in this study was 33, which fell to 15, as shown in Table 2.
5.5.2. Domain Validity

Of the 15 domains obtained from the literature, as well as previous content and panel validity tests, only 10 were included in the final model, as shown in Table 3.

| Domains Selected from the Literature | Domains Selected by Field Evaluators | Domains Selected According to SEM |
|-------------------------------------|-------------------------------------|-----------------------------------|
| 1 Information security compliance behavior (ISCB) | ✓ | ✓ |
| 2 Self-efficacy | ✓ | ✓ |
| 3 Subjective norms | ✓ | ✓ |
| 4 Attitude towards information system security policy (ISSP) compliance | ✓ | |
| 5 Response efficacy | ✓ | |
| 6 Response cost | ✓ | |
| 7 Perceived vulnerability | ✓ | |
| 8 Perceived severity | ✓ | |
| 9 General information security | ✓ | ✓ |
| 10 Technology awareness | ✓ | ✓ |
| 11 ISSP awareness | ✓ | |
| 12 Normative beliefs | ✓ | |
| 13 Perceived cost of compliance | ✓ | ✓ |
| 14 Work impediment | ✓ | |
| 15 Intrinsic benefit | ✓ | |
| 16 Rewards | ✓ | |
| 17 Safety of resources | ✓ | |
| 18 Perceived benefit of compliance | ✓ | |
| 19 Sanctions | ✓ | |
| 20 Vulnerability of resources | ✓ | |
| 21 Perceived cost of non-compliance | ✓ | |
| 22 Information security policy | ✓ | ✓ |
| 23 Information security policy provision | ✓ | |
| 24 SETA programs | ✓ | |
| 25 IT knowledge | ✓ | |
| 26 Negative experience | ✓ | |
| 27 Influence of secondary sources | ✓ | |
| 28 Peer behavior | ✓ | |
| 29 Risky behavior | ✓ | |
| 30 Attitude towards cyber security | ✓ | |
| 31 Legal consequences/punishment | ✓ | ✓ |
| 32 Religion and morality | ✓ | ✓ |
| 33 Personality traits (extraversion, agreeableness, conscientiousness, neuroticism, intellect/imagination) | ✓ | ✓ |

5.5.3. Hypothetical Dimensions, Statistical Validity, and Reliability

Partial least squares (PLS-SEM) was used to test the dimensions and identify the path coefficients (Figure 1). According to the requirements for approving the dimensions of the theoretical model, three values must be within the standards, namely the t-values (path coefficients), significance, and goodness of fit. Since the t-values of dimensions were greater than 1.96, they were deemed to be the main valid dimensions of ISCB. As mentioned by Kim et al. [17] and Chin et al. [34], the best goodness of fit for any model in PLS-SEM should be classified as low, middle, or high. The ranges for each category are 0.02 ≤ R² ≤ 0.13, 0.13 ≤ R² ≤ 0.26, and above 0.26 for the low, middle, and high forecasting goodness of fit, respectively. High-ranging R squared values of the present theoretical model were observed in the influence of personality traits, followed by technology awareness, subjective norms, general information security, information security policy, legal punishment, and compliance/noncompliance cost. Mid-level
R squared values were observed for the effect of self-efficacy and religion on ISCB. The overall goodness of fit for this model achieved about 78% (R squared = 0.780), as shown in Figure 1. Therefore, this model is considered to meet the requirements for employee ISCB in Saudi Arabia. Additionally, statistical validity was performed by using confirmatory and exploratory factor analysis. Cronbach’s alpha was used to determine the internal consistency of questions and variables as one set. Reliability values were found to be 0.942 for ISCB, 0.937 for subjective norms, 0.901 for self-efficacy, 0.868 for religion and morality, 0.876 for personality traits, 0.893 for general information security, 0.984 for information security policy, 0.866 for legal consequences/punishment, 0.789 for the perceived cost of compliance/non-compliance, and 0.858 for technology awareness. The overall Cronbach’s alpha for the survey was 0.936. After factor analysis was conducted, sixty-two survey items were retained across domains. They were distributed as follows: 9 on religion/morality, 8 on legal consequences/punishment, 10 on the Big-Five personality traits, 9 on ISCB, 10 on self-efficacy, 4 on subjective norms, 3 on the cost of compliance/non-compliance, 3 on general information security, 2 on information security policy, and 4 on technology awareness.

Figure 1. Model and domains of information security compliance behavior (ISCB) generated by SmartPLS.

5.6. Second Phase and Prediction Analysis

5.6.1. Dependent and Independent Variables

However, the present study aimed to identify the impact of other non-common variables, such as religion, punishment, and personality traits, alongside the common theories. Figure 2 depicts the influence of independent and moderator variables (as identified by existing theories) on the dependent variable. The study’s independent and moderator variables include legal consequences/punishment (GDT), personality traits and self-efficacy (PMT), cost of compliance/non-compliance (rational choice theory (RCT)), subjective norms (TPB), religion and morality (cognitive moral development theory), and information security policy, general information security, and technology awareness (DOI). Demographic characteristics were the only controlled variable.
5.6.2. Hypotheses of Variables in the Main Study

The hypotheses of the present study are classified into common, non-common, moderators, and demographic effects. The corresponding abbreviations and explanations of these hypotheses are as follows. H01: There are no predictors of ISCB among healthcare employees in the KSA. H02: Non-common factors (e.g., religion/morality, personality traits, and legal consequences/punishment) have no effect on ISCB among healthcare employees in the KSA. H03: Moderators have no effect on ISCB among healthcare employees in the KSA. H04: Demographic characteristics have no impact on ISCB among healthcare employees in the KSA.
As shown in Figure 3, null hypotheses concerning religion/morality, legal consequences/punishment, and personality traits are abbreviated as H02R, H02LP, and H02P, respectively. Null hypotheses concerning subjective norms, self-efficacy, cost of compliance/non-compliance, technology awareness, general information security, and information security policy are abbreviated as H01SN, H01SE, H01CC, H01TA, H01GIS, and H01ISP, respectively. Hypothesis 3 relates to moderators, and Hypothesis 4 refers to the effects of demographics on ISCB.

6. Results and Analysis

The response rate of participants for this survey was 62.1%, which is considered an excellent rate, especially amidst the inconvenient health conditions of the COVID-19 pandemic. Of the surveys, eleven-point-five percent were considered as incomplete and were excluded from the study, while 26.4% provided no response. Participants’ responses on ISCB and its domains were recorded in terms of percentages and frequencies. Predictors of ISCB were determined, and those with the highest impact were considered. In addition, the moderating influence of their interactions on ISCB scores was measured. Finally, the factors affecting the main domains of ISCB were examined.

6.1. Demographic Characteristics

The average age of participants was 33.2 years. Table 4 details the percentages of every category according to the demographic characteristics of participants. The majority of participants’ characteristics were male (53.10%), married (80.10%), with a BSc degree (40.90%), 6–10 years’ work experience (33.90%), nurse specialty (42.50%), and work location at the Al-Amal Center (22.20%).

| Characteristic | Category | Result | Characteristic | Category | Result |
|----------------|----------|--------|----------------|----------|--------|
| Gender         | Male     | 53.10% | Specialty      | Nurse    | 42.50% |
|                | Female   | 46.90% | Administrator  | Pharmacists | 42.50% |
| Marital status | Married  | 80.10% | Physicians     | 3.50%    |
|                | Single   | 15.50% | Other          | 29.30%   |
|                | Divorced | 3.70%  |                |          |
|                | Others   | 0.70%  |                |          |
| Education      | BSc      | 40.90% | Work location  | Al-Amal Centre | 22.20% |
|                | Diploma  | 43%    | Central Hospital | 15.20%  |
|                | Higher education | 7.60% | Al-Riaya Hospital | 14.30% |
|                | Secondary school | 7.90% | Prince Abdulazizi Hospital | 12.00% |
|                | Others   | 0.70%  | Obstetrics and Pregnancy Hospital | 8.10% |
| Work experience| <1 year  | 11.10% | Other          | 28.20%   |
|                | 1–5 years| 17.3%  |                |          |
|                | 6–10 years| 33.9% |                |          |
|                | 10–15 years| 20.6% |                |          |
|                | >15 years| 17.10% |                |          |

6.2. Participants’ Responses

Appendix A lists participant responses to a number of statements within each examined domain. Answers were provided on a five-point Likert scale ranging from: strongly agree (SA) to agree (A), neither agree, nor disagree (N), disagree (D), and strongly disagree (SD). Statements were selected for inclusion in the table below according to two relevance criteria within each domain: (a) high level of overall agreement on the Likert scale (i.e., most people answered A or SA) and (b) high mean level of agreement. For instance, in the “religion and morality” domain, the selection of “SA” had the highest score (54.43%). The response of A by participants towards ISCB was 52.48%. The response of participants towards punishment, self-efficacy, subjective norms, cost of compliance/noncompliance, general information security, information security policy, technology awareness, and personality was mostly A (42.21%, 49.45%, 42.09%, 37.57%, 50.04%, 48.73%, 47.86%, and 44.85%, respectively), as outlined in Appendix A.
6.3. Predictors of ISCB

Multiple linear regression (dummy method) was used to determine ISCB predictors among study participants. Calculated ISCB predictor values are shown in Table 5. The proposed model was found to have a predictive value of approximately 60% (adjusted R² = 0.595), which indicates a relatively high goodness of fit. General information security had the greatest positive effect on the ISCB model (β = 0.250), followed by self-efficacy (β = 0.223), religion/morality (β = 0.217), personality traits (β = 0.166), subjective norms (β = 0.152), and legal consequences/punishment (β = 0.147). However, the extent of positive increments in the ISCB score was highest for general information security (B = 0.603), i.e., increasing one unit of general information security yields an increase in the ISCB score by 60.3%. This effect is followed by personality traits (33.5%, B = 0.335), subjective norms (26.3%, B = 0.263), religion/morality (23.7%, B = 0.237), self-efficacy (17.8%, B = 0.178), and legal consequences/punishment (13.9%, B = 0.139). The final ISCB model achieved about 59.5% and is thus considered a good model to describe employee perceptions in Saudi Arabian health settings. This result is slightly lower than the value obtained in the theoretical model during the first phase of theoretical modeling. This indicates that there is a slight difference in determining the domains of ISCB between the theory and actual settings.

### Table 5. Predictors of ISCB.

| Predictors                        | Unstandardized Coefficient | Standardized Coefficient | t     | Sig. | 95.0% CI for B |
|----------------------------------|---------------------------|--------------------------|-------|------|----------------|
| (Constant)                       | −6.028                    |                          | −2.408| 0.017| −10.95, −1.106 |
| Religion/morality                | 0.237                     | 0.217                    |       | <0.001| 0.161, 0.313 |
| Personality traits               | 0.315                     | 0.166                    | 4.794 | <0.001| 0.198, 0.472 |
| Legal consequences/punishment    | 0.139                     | 0.147                    | 3.704 | <0.001| 0.065, 0.213 |
| Self-efficacy                    | 0.178                     | 0.223                    | 4.939 | <0.001| 0.107, 0.249 |
| Subjective norms                | 0.263                     | 0.152                    | 3.601 | <0.001| 0.119, 0.406 |
| General information security     | 0.603                     | 0.250                    | 5.480 | <0.001| 0.386, 0.819 |

Multiple linear regression: R² = 0.775 (adjusted R² = 0.595), df (6), p < 0.001.

Based on the above results, the null hypotheses H01 (there are no predictors of ISCB among healthcare employees in the KSA) and H02 (non-common factors such as religion/morality, personality traits, and legal consequences/punishment have no effect on ISCB among healthcare employees in the KSA) can be rejected.

6.4. Moderators of ISCB

Table 6 illustrates the impact of moderators on ISCB. Information security policy and technology awareness only showed significant effect, where the impact on the ISCB as the Beta value is equal to 0.642 of the model. The low value of the R squared of moderators can be attributed to the use of the dummy method of regression, as this method generally showed low R squared values when using a small number of variables in the same model. However, about 35% was obtained for the moderating effect of information security policy and technology awareness on the ISCB. Interestingly, the t-value obtained from the regression model showed a good relationship between the moderating effects of these variables on the ISCB. Based on the above results, null hypothesis H03 (information security policy and technology awareness have a moderating impact on ISCB among healthcare employees in the KSA) can be rejected.
Table 6. Impact of domain interaction on information security compliance behavior (ISCB).

| Predictors                                      | Unstandardized Coefficient | Standardized Coefficient | t     | Sig. | 95.0% CI for B |
|-------------------------------------------------|----------------------------|--------------------------|-------|------|----------------|
| Constant                                        | 28.814                    | 2.805                    | 10.272| <0.001 | 23.299 34.330  |
| Information security policy and technology     |                            |                          |       |      |                |
| awareness                                      |                            |                          |       |      |                |
| Information security policy                     | −0.356                    | 0.429                    | −0.111| −0.830| 0.407 0.487    |
| Technology awareness                            | 0.095                     | 0.210                    | 0.058 | 0.452| 0.652 0.508    |
| Technology awareness * Information security    | 0.077                     | 0.026                    | 0.642 | 2.912| 0.004 0.129    |
| policy                                         |                            |                          |       |      |                |

* Multiple linear regression: \(R^2 = 0.596\) (adjusted \(R^2 = 0.350\)), df (3), \(p < 0.001\).

6.5. Final Model of ISCB

In line with the fifth objective of this study, namely to present a final theory-based model of ISCB among healthcare workers in the KSA, Figure 4 depicts the relevant domains. Regression models were run, and Beta coefficient values were used to determine the impacts of these domains on ISCB. General information security had the highest impact, followed by self-efficacy, religion/morality, personality traits, subjective norms, and legal/punishment. Influences of other factors are also stated, with the significant results of these variable among each. For example, legal/punishment influences self-efficacy only. Personality weakly influences self-efficacy. Therefore, the non-common factors may directly influence ISCB.

![Figure 4](image)

Figure 4. Model and predictors of ISCB among healthcare workers in the KSA NS = not significant.

7. Discussion

Models have previously been formulated to detect and manage violations of information security systems. They have been implemented to identify factors commonly associated with the weaknesses of healthcare systems, such as technical problems, personal problems, security architecture, information security governance, and business and recovery planning [35–37]. Several Saudi studies have attempted to determine the factors influencing information security systems, especially those related to employee behavior, but were either categorized as review studies or deemed methodologically insufficient [38,39]. This paper aims to bridge this research gap by formulating an integral model of the broad dimensions influencing ISCB among employees at governmental healthcare centers in Arar City, KSA. Some scholars have highlighted the influence of psychological parameters on
the protection of information technology systems at hospitals [9]. However, these psychological parameters vary in nature based on type, severity, risk, and the relationship to violation of information security of healthcare professionals at medical institutions. All of these variables are particular to the requirements of specific theories and policies when creating models of ISCB. Kim et al. [17] proposed a hybrid model derived from four theories: TPB, RCT, naturalization theory, and PMT. Along those lines, the present study examines several dimensions that directly and indirectly affect ISCB among healthcare employees in the KSA. Moreover, the country’s unique culture has impacted employees’ psychological and information security behavior in domains such as religion, personality, and commitment to legal consequences [12]. The proposed model constitutes a novel addition to the literature, especially as it combines psychological, technical, management, and cultural parameters involved in ISCB. Kim et al. [17] proposed self-efficacy as one of the variables that may be influenced by ISCB. However, they found no significant impact of self-efficacy on ISCB. The present study demonstrates a significant impact of self-efficacy on ISCB, with better association results ($\beta = 0.223$) than their outcome. The value of self-efficacy in the present study is similar to previous outcomes [31]. The controversial results about the impact of self-efficacy on information security behavior are probably due to the inconsistency of the definition, use, and measurement of the level of self-efficacy and the method of evaluating the relationship within the context of security behavior [40]. For this reason, the present study passes through several precise methodological and validation steps to define the items and scales of self-efficacy. Klein et al. detected the relationship between punishment severity and security behavior. Unfortunately, although they stated the importance of punishment and severity, no significant relationship could be observed [41]. Ryutov et al. [9] noticed the substantial association between severity of punishment and security compliance behavior, with a regression coefficient of 0.132. Remarkably, the present study reveals a significant association between punishment/legal predictor and ISCB, almost similar to the outcomes obtained by [9]. Therefore, punishment/legal concerns are considered as an exclusive result, and a new domain should be considered when conducting future research, especially in the context of Saudi Arabian culture. A previous study found that religious and moral factors are strong predictors of commitment to self-improvement and personal behavior [42]. Bansal et al. also found an association between the non-compliance of employees with religious/moral beliefs, where a significantly negative relationship was observed between negative compliance and high levels of morality/religiosity. Kurpis et al. found that the standardized coefficient, implying the strength of the relationship, of the religiosity factor significantly influenced the intention and compliance behavior, with a value of 0.234 [42]. This result is in line with the outcomes of the present study, where the regression standardized coefficient ($\beta = 0.217$) is significantly influenced by the ISCB of healthcare employees of the governmental hospitals and clinical centers in Arar, KSA. This outcome is considered to answer many researchers’ questions concerning the impact of religion/moral beliefs on the information security behavior of healthcare workers, particularly in countries with specific environments like that of the KSA [12]. Establishing the significant relationship between religion and security behavior is considered as another novelty of the present study, as this new dimension (religion/morality) should be considered in future studies conducted in the KSA. The assessment of personality has received the attention of several researchers, especially regarding its relationship with information security and social behavior. Vance et al. confirmed this association and the impact of personality on the failure or success of employees at protecting patients’ confidential information. Moreover, they attributed the influence of personality to protection motivation and habit theories [43]. All studies conducted in Saudi Arabia lacked a systematic and broad view of the common domains that influence the culture, such as personality traits, which may differ in each region of the country, or from nearby countries [12]. This privileged the present study to highlight the common psychological and habitual parameters that influence behavior in Saudi Arabian culture. Kim et al. [17] categorized subjective norms as one of the three social psychological parameters, in addition to attitude and perceived control, which influence information security behavior within planned action and behavior theory. Subjective norms, as reported by a previous study, encourage someone to do certain things
under pressure, which reveals the extent of compliance to rules [44]. Ryutov et al. [9] investigated the impact of subjective norms on the ISCB, but they could not observe significance in their hypothesis. Borena and Bélanger [45] justified the nonsignificant result of their hypothesis on subjective norms and information security behavior by citing the lack of a direct effect. This opinion is rejected by the present study and in studies conducted by Herath and Rao [32]. Borena and Bélanger [45] found a significant association between subjective norms and ISCB, with a coefficient equal to 0.313 [45]. Their subjective norm value supports the findings of the present study. Haessinger and Kranz [46] found that general information security awareness significantly influences security awareness and thus security behavior. This view supports the model of the present study, where the general information security variable directly influences information security compliance behavior ($\beta = 0.250$). Regarding research related to the outcome of this study, no previous studies have revealed the value of their coefficients, despite the significant influence of general information awareness on ISCB. In general, most studies found in the literature have formulated their theoretical models without taking into consideration co-factors such as moderators and socio-demographic characteristics. However, these were investigated in the present study, which is considered a novel achievement for predictors of ISCB for Saudi Arabian healthcare workers.

8. Conclusions and Future Work

The adoption of HISs by healthcare organizations offers several benefits, such as improved service quality, the reduction of medical errors, and greater accessibility of information. The government of the KSA has subsidized this field to keep pace with developed countries. However, like those of other less developed nations, organizations in the KSA struggle to secure their HISs. This stems from a number of factors, including a lack of awareness of information security and technological barriers. Most existing studies do not consider all factors affecting information security compliance, which include psychological traits, cultural beliefs, religion, and legal concerns. This paper investigates the usefulness of the proposed model in determining the predictors of information security compliance among healthcare workers at governmental hospitals in the KSA. It is conducted on 433 healthcare personnel at five key hospitals and health centers in Arar, the capital of the Northern Border Province. To strengthen the results, multiple validation tests (e.g., content validity and panel validity tests) are conducted on the study’s instruments. In addition, statistical tests are run on the data collected from participants. The results indicate an impact of moderators and non-common factors (e.g., religion and morality) on ISCB. However, demographic characteristics (e.g., age, marital status, and work experience) appear to have no impact. This theory-based model of ISCB among healthcare workers could be useful in similar contexts. The present study presents a significant model of ISCB and significant predictors on the theoretical and practical observational levels. Risk factors of ISCB obtained in present study are religion/morality, personality traits, legal consequences/punishment, self-efficacy, subjective norms, and general information security. The moderating impact of information security policy and technology awareness significantly influence the ISCB of employees in the KSA. This study possesses some limitations, which invite future research in the area. First, its cross-sectional design has weaknesses in certain research aspects, including time and updating of knowledge and experience about information security. Second, the study should extend beyond governmental healthcare centers and hospitals in a single Saudi city (i.e., Arar), to include private hospitals and other areas of the KSA.

Author Contributions: Conceptualization: S.T.A., M.A., S.A.E. and H.A.A.-A.; Formal analysis: S.T.A., S.A.E. and H.A.A.-A.; Funding acquisition: M.A. and S.K.; Investigation: S.T.A.; Project administration: M.A.; Software: H.A.A.-A.; Supervision: M.A., S.A.E. and S.K.; Writing—original draft: S.T.A. and S.A.E.; Writing—review & editing: S.T.A., M.A. and S.A.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.
### Appendix A

**Table A1.** Responses of information security compliance behavior (ISCB) and domains after factor analysis.

|                                           | SD  | D   | N   | A   | SA  | M   | ±SD |
|-------------------------------------------|-----|-----|-----|-----|-----|-----|-----|
| **Religion and moral**                    |     |     |     |     |     |     |     |
| 1. My religious faith is extremely important to me | 5   | 2   | 10  | 159 | 257 | 4.53| 0.680 |
|                                           | 1.2 | 0.5 | 2.3 | 36.7| 59.4|     |     |
| 2. I pray daily                           | 2   | 0   | 19  | 164 | 248 | 4.52| 0.628 |
|                                           | 0.5 | 0   | 4.4 | 37.9| 57.3|     |     |
| 3. I look to my faith as a source of inspiration | 4   | 3   | 21  | 167 | 238 | 4.46| 0.706 |
|                                           | 0.9 | 0.7 | 4.8 | 38.6| 55  |     |     |
| 4. I look to my faith as providing meaning and purpose in my life | 5   | 1   | 19  | 178 | 230 | 4.45| 0.699 |
|                                           | 1.2 | 0.2 | 4.4 | 41.1| 53.1|     |     |
| 5. My faith is an important part of who I am as a person | 4   | 1   | 28  | 166 | 234 | 4.21| 0.755 |
|                                           | 0.9 | 0.2 | 6.5 | 38.3| 54  |     |     |
| 6. I consider myself active in my faith or at mosque | 3   | 8   | 45  | 215 | 162 | 4.44| 0.709 |
|                                           | 0.7 | 1.8 | 10.4| 49.7| 37.4|     |     |
| 7. My relationship with God is extremely important to me. | 4   | 0   | 11  | 145 | 273 | 4.58| 0.638 |
|                                           | 0.9 | 0.7 | 4.8 | 33.5| 63  |     |     |
| 8. I look to my faith as a source of comfort | 3   | 3   | 21  | 146 | 260 | 4.52| 0.687 |
|                                           | 0.7 | 0.7 | 4.8 | 33.7| 60  |     |     |
| 9. My faith impacts many of my decisions | 15  | 8   | 37  | 154 | 219 | 4.28| 0.949 |
|                                           | 3.5 | 1.8 | 8.5 | 35.6| 50.6|     |     |
| **Total no.**                             | 45  | 26  | 211 | 1494| 2121|     |     |
| **Legal and punishment**                  |     |     |     |     |     |     |     |
| %                                        | 1.15 | 0.67 | 5.41 | 38.34 | 54.43 | 3.78 | 0.939 |
| 1. My hospital has clear, written policies and procedures related to employee discipline. | 14  | 19  | 108 | 200 | 92  | 3.78 | 0.939 |
|                                           | 3.2 | 4.4 | 24.9| 46.2| 21.2|     |     |
| 2. I believe that employee non-compliance can usually be corrected with punishment | 14  | 26  | 98  | 206 | 89  | 3.76 | 0.953 |
|                                           | 3.2 | 6   | 22.6| 47.6| 20.6|     |     |
| 3. I believe that most non-compliant employees are eventually terminated | 52  | 73  | 123 | 124 | 57  | 3.14 | 1.205 |
|                                           | 12  | 17.3| 28.9| 28.6| 13.2|     |     |
| 4. I believe that trust between supervisors and "direct reports" is important in improving employee compliance | 5   | 8   | 61  | 195 | 164 | 4.17 | 0.819 |
|                                           | 1.2 | 1.8 | 14.1| 45  | 37.9|     |     |
|                  | SD  | D   | N   | A   | SA  | M  | ±SD |
|------------------|-----|-----|-----|-----|-----|----|-----|
| **Legal and**    |     |     |     |     |     |    |     |
| **punishment**   |     |     |     |     |     |    |     |
| 5. I believe that most of our supervisors and managers utilize verbal warnings to improve the compliance of their employees | 14  | 20  | 81  | 211 | 107 | 3.87| 0.946 |
|                  | 3.2 | 4.6 | 18.7| 48.7| 24.7|    |     |
| 6. I believe that most of our supervisors and managers use written behavior counseling with their non-compliant employees | 19  | 28  | 118 | 178 | 90  | 3.67| 1.015 |
|                  | 4.4 | 6.5 | 27.3| 41.1| 20.8|    |     |
| 7. I believe that most of our supervisors and managers use written behavior contracts with their non-compliant employees | 18  | 36  | 115 | 175 | 89  | 3.65| 1.028 |
|                  | 4.2 | 8.3 | 26.6| 40.4| 20.6|    |     |
| 8. Managers and supervisors are given latitude to apply hospital policies and procedures related to employee discipline | 26  | 34  | 114 | 173 | 86  | 3.60| 1.076 |
|                  | 6   | 7.9 | 26.3| 40  | 19.9|    |     |
| **Personality traits** |     |     |     |     |     |    |     |
| 1. Am relaxed most of the time | 4.68 | 7.10 | 23.67 | 42.21 | 22.34 |    |     |
|                  | 1.8 | 6.5 | 20.3 | 52.9 | 18.5 |    |     |
| 2. Get upset easily | 58  | 96  | 97  | 135 | 47  | 3.04| 1.227 |
|                  | 13.4| 22.2| 22.4| 31.2| 10.9|    |     |
| 3. Talk to a lot of different people at parties | 11  | 34  | 99  | 204 | 85  | 3.73| 0.948 |
|                  | 2.5 | 7.9 | 22.9 | 47.1| 19.6|    |     |
| 4. Have a vivid imagination | 10  | 30  | 101 | 194 | 98  | 3.79| 0.949 |
|                  | 2.3 | 6.9 | 23.3 | 44.8| 22.6|    |     |
| 5. I Am not interested in abstract ideas | 20  | 66  | 135 | 165 | 47  | 3.35| 1.015 |
|                  | 4.6 | 31.2| 38.1| 10.9|     |    |     |
| 6. I Have difficulty understanding abstract ideas | 37  | 92  | 124 | 133 | 47  | 3.14| 1.131 |
|                  | 8.5 | 21.2| 28.6| 30.7| 10.9|    |     |
| 7. A Sympathize with others' feelings | 2   | 10  | 75  | 233 | 113 | 4.03| 0.754 |
|                  | 0.5 | 2.3 | 17.3 | 53.8| 26.1|    |     |
| 8. Feel others' emotions | 5   | 10  | 75  | 227 | 116 | 4.01| 0.799 |
|                  | 1.2 | 2.3 | 17.3 | 52.4| 26.8|    |     |
| 9. Get chores done right away | 3   | 8   | 60  | 224 | 138 | 4.12| 0.762 |
|                  | 0.7 | 1.8 | 13.9| 51.7| 31.9|    |     |
| 10. Like order   | 3   | 9   | 62  | 198 | 161 | 4.17| 0.796 |
|                  | 0.7 | 2.1 | 14.3| 45.7| 37.2|    |     |
| **Total no.**    | 157 | 383 | 916 | 1942| 932 |    |     |
| **%**            | 3.63| 8.85| 21.15| 44.85| 21.52|    |     |
| Information security compliance behavior | SD   | D   | N   | A   | SA  | M   | ±SD  |
|-----------------------------------------|------|-----|-----|-----|-----|-----|------|
| It is my intention to continue to comply with the organization’s ISSP | 1.2  | 7   | 85  | 221 | 615 | 4.00| 0.795|
| I am certain I will adhere to my organization’s ISSP | 0.9  | 10  | 57  | 228 | 134 | 4.10| 0.779|
| It is possible that I will comply with the organization’s ISSP to protect the organization’s information systems | 2.8  | 11  | 61  | 222 | 127 | 4.02| 0.887|
| I am likely to follow the organization’s ISSP in the future | 1.2  | 6   | 64  | 231 | 127 | 4.08| 0.771|
| I would follow the organization’s security policy whenever possible | 1.8  | 6   | 57  | 224 | 138 | 4.10| 0.814|
| I intend to protect technology resources according to the requirements of the ISSP of my organization | 2.3  | 4   | 59  | 222 | 138 | 4.09| 0.832|
| I intend to carry out my responsibilities prescribed in the ISSP of my organization when I use information resources | 2.3  | 6   | 63  | 234 | 127 | 4.10| 0.74 |
| I intend to carry out my responsibilities prescribed in the ISSP of my organization when I use technology resources | 1.4  | 6   | 57  | 224 | 138 | 4.10| 0.769|
| I intend to recommend that others comply with ISSP | 1.4  | 10  | 58  | 566 | 2045 | 1165 |
| Total no. | 63   | 58  | 566 | 2045 | 1165 |

| Self-efficacy | SD  | D  | N  | A  | SA | M  | ±SD  |
|---------------|-----|----|----|----|----|----|------|
| 1. I have the necessary skills to protect myself from information security violations | 1.62| 1.49| 14.52| 52.48| 29.89| 3.97| 0.827|
| 2. I have the expertise to implement preventative measures to stop people from getting my confidential information | 2.1| 1.8| 17.8| 53.8| 24.5|               |
| 3. I have the skills to implement preventative measures to stop people from damaging my work computer | 1.6| 2.8| 18.5| 50.3| 26.8|               |
| 4. I can enable security measures on my work computer but only when I have manuals for reference | 2.8| 10| 94| 196| 117| 3.86| 0.944|
| 5. I have the necessary skills to fulfill the requirements of the ISP | 2.3| 2.3| 21.9| 48.3| 25.4|               |
| 6. I have the necessary knowledge to fulfill the requirements of the ISP | 2.1| 3.9| 22.9| 48.7| 22.4|               |
### Table A1. Cont.

| Self-efficacy                                                                 | SD | D | N | A | SA | M | ±SD |
|--------------------------------------------------------------------------------|----|---|---|---|----|---|-----|
| 7. I have the necessary competencies to fulfill the requirements of the ISP    | 4  | 19 | 99 | 211 | 100 | 3.89 | 0.841 |
|                                                                                 | 0.9 | 4.4 | 22.9 | 48.7 | 23.1 |       |     |
| 8. I would feel comfortable following my organization’s ISSP on my own         | 3  | 11 | 71 | 224 | 124 | 4.05 | 0.783 |
|                                                                                 | 0.7 | 2.5 | 16.4 | 51.7 | 28.6 |       |     |
| 9. If I wanted to, I could easily comply with my organization’s ISSP on my own| 3  | 8  | 90 | 223 | 109 | 3.99 | 0.773 |
|                                                                                 | 0.7 | 1.8 | 20.8 | 51.5 | 25.2 |       |     |
| 10. I would be able to follow most of ISSP even if there was no one around to help me | 5  | 17 | 96 | 202 | 113 | 3.93 | 0.860 |
|                                                                                 | 1.2 | 3.9 | 22.2 | 46.7 | 26.1 |       |     |
| Total no.                                                                      | 74 | 137 | 897 | 2141 | 1081 |       |     |
| %                                                                              | 1.71 | 3.16 | 20.72 | 49.45 | 24.97 |       |     |

| Subjective norms                                                               | SD | D | N | A | SA | M | ±SD |
|--------------------------------------------------------------------------------|----|---|---|---|----|---|-----|
| 1. My organization’s IT department pressures me to follow the organization’s ISSP | 28 | 48 | 150 | 163 | 44 | 3.34 | 1.020 |
|                                                                                 | 6.5 | 11.1 | 34.6 | 37.6 | 10.2 |       |     |
| 2. My subordinates think I should follow the organization’s ISSP                | 13 | 23 | 145 | 191 | 61 | 3.61 | 0.899 |
|                                                                                 | 3  | 5.3 | 33.5 | 44.1 | 14.1 |       |     |
| 3. Upper level management thinks I should comply with the requirements of my organization’s ISPPs | 14 | 23 | 134 | 189 | 73 | 3.66 | 0.930 |
|                                                                                 | 3.2 | 5.3 | 30.9 | 43.6 | 16.9 |       |     |
| 4. My colleagues think that I should comply with the requirements of my organization’s ISPPs | 14 | 22 | 146 | 186 | 65 | 3.61 | 0.914 |
|                                                                                 | 3.2 | 5.1 | 33.7 | 43.0 | 15.0 |       |     |
| Total no.                                                                      | 69 | 116 | 575 | 729 | 243 |       |     |
| %                                                                              | 3.98 | 6.70 | 33.20 | 42.09 | 14.03 |       |     |

| Cost of compliance/ noncompliance                                               | SD | D | N | A | SA | M | ±SD |
|--------------------------------------------------------------------------------|----|---|---|---|----|---|-----|
| 1. My noncompliance with the requirements of the ISSP would impact me negatively | 21 | 28 | 127 | 190 | 67 | 3.59 | 0.987 |
|                                                                                 | 4.8 | 6.5 | 29.3 | 43.9 | 15.5 |       |     |
| 2. Complying with the requirements of the ISSP is time consuming for me         | 25 | 68 | 145 | 152 | 43 | 3.28 | 1.030 |
|                                                                                 | 5.8 | 15.7 | 33.5 | 35.1 | 9.9 |       |     |
| 3. Complying with the requirements of the ISSP is burdensome for me             | 40 | 64 | 141 | 146 | 42 | 3.20 | 1.098 |
|                                                                                 | 9.2 | 14.8 | 32.6 | 33.7 | 9.7 |       |     |
| Total no.                                                                      | 86 | 160 | 413 | 488 | 152 |       |     |
| %                                                                              | 6.62 | 12.32 | 31.79 | 37.57 | 11.70 |       |     |
| General information security                                      | SD  | D  | N  | A  | SA | M  | ±SD |
|------------------------------------------------------------------|-----|----|----|----|----|----|-----|
| 1. Overall, I am aware of the potential security threats and their negative consequences | 8.0| 14 | 79 | 216| 116| 3.97| 0.864|
|                                                                  | 1.8| 3.2| 18.2| 49.9| 26.8|     |     |
| 2. I have sufficient knowledge about the cost of potential security problems | 6.0| 15 | 95 | 215| 102| 3.91| 0.843|
|                                                                  | 1.4| 3.5| 21.9| 49.7| 23.6|     |     |
| 3. I understand the concerns regarding information security and the risks they pose in general | 7.0| 12 | 84 | 219| 111| 3.96| 0.841|
|                                                                  | 1.6| 2.8| 19.4| 50.6| 25.6|     |     |
| Total no.                                                        | 21  | 41 | 258| 650| 329|     |     |
| %                                                                | 1.62| 3.16| 19.86| 50.04| 25.33|     |     |
| Information security policy                                      | SD  | D  | N  | A  | SA | M  | ±SD |
| 1. I understand the rules and regulations prescribed by the ISSP of my organization | 15  | 17 | 99 | 212| 90 | 3.80| 0.931|
|                                                                  | 3.5 | 3.9| 22.9| 49.0| 20.8|     |     |
| 2. I know my responsibilities as prescribed in the ISSP to enhance the IS security of my organization | 11  | 22| 94 | 210| 96 | 3.83| 0.918|
|                                                                  | 2.5 | 5.1| 21.7| 48.5| 22.2|     |     |
| Total no.                                                        | 26  | 39 | 193| 422| 186|     |     |
| %                                                                | 3.00| 4.50| 22.29| 48.73| 21.48|     |     |
| Technology awareness                                             | SD  | D  | N  | A  | SA | M  | ±SD |
| 1. I follow news and developments about the security related technologies | 13  | 32 | 107| 201| 80 | 3.70| 0.954|
|                                                                  | 3   | 7.4| 24.7| 46.4| 18.5|     |     |
| 2. I discuss Internet security issues or anecdotes with friends and people around me | 12  | 17 | 115| 210| 79 | 3.76| 0.892|
|                                                                  | 2.8 | 3.9| 26.6| 48.5| 18.2|     |     |
| 3. I read about the problems of malicious threats attacking users' computers | 14  | 22 | 98 | 219| 82 | 3.77| 0.918|
|                                                                  | 3.2 | 22.6| 50.6| 18.9|     |     |
| 4. I seek advice about security issues through online discussion forums, magazines, and other media sources | 19  | 22 | 106| 199| 87 | 3.72| 0.985|
|                                                                  | 4.4 | 5.1| 24.5| 46 | 20.1|     |     |
| Total no.                                                        | 58  | 91 | 426| 829| 328|     |     |
| %                                                                | 3.35| 5.25| 24.60| 47.86| 18.94|     |     |
References

1. Lingamallu, K.; Nayakvadi, S. Role of HIS and RIS in Improving Quality of Patient Care. *Int. J. Collab. Res. Intern. Med. Public Health* 2018, 10, 725–734.

2. Ebad, S.A.; Jaha, E.S.; Al-Qadhi, M.A. Analyzing privacy requirements: A case study of healthcare in Saudi Arabia. *Informatics Health Soc. Care* 2016, 41, 47–63. [CrossRef] [PubMed]

3. AlKalbani, A.; Deng, H.; Kam, B.; Zhang, X. Information Security compliance in organizations: An institutional perspective. *Data Inf. Manag.* 2017, 1, 104–114. [CrossRef]

4. Hwang, I.; Wakefield, R.; Kim, S.; Kim, T. Security Awareness: The First Step in Information Security Compliance Behavior. *J. Comput. Inf. Syst.* 2019, 1–12. [CrossRef]

5. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q.* 2010, 34, 523–548. [CrossRef]

6. Shaban, M.H. The Influence of Malicious Human Factors on Information System Security in Iraq Hospitals. Ph.D. Thesis, Universiti Teknologi Malaysia, Johor Bharu, Malaysia, 2015.

7. Hawthorne, K.H.; Richards, L. Personal health records: A new type of electronic medical record. *Rec. Manag. J.* 2017, 27, 286–301. [CrossRef]

8. Mishah, N.; Bukhari, A.; AlMutairi, B.; Mohreq, M. Status of e-security and privacy protection in Saudi hospitals. *Comput. Methods Progr. Biomed.* 2019, 171, 5–6. [CrossRef]

9. Ryutov, T.; Sintov, N.; Zhao, M.; John, R.S. Predicting information security policy compliance intentions and behavior for six employee-based risks. *J. Inf. Priv. Secur.* 2017, 13, 260–281.

10. Siponen, M.; Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Q.* 2010, 34, 487–502. [CrossRef]

11. Menachemi, N.; Collum, T.H. Benefits and drawbacks of electronic health record systems. *Risk Manag. Healthc. Policy* 2011, 4, 47. [CrossRef]

12. Alkahtani, H.K. Raising the information security awareness level in Saudi Arabian organizations through an effective, culturally aware information security framework. Ph.D. Thesis, Loughborough University, Reading, UK, 2018.

13. Box, D.; Pottas, D. Improving information security behavior in the healthcare context. *Procedia Technol.* 2013, 9, 1093–1103. [CrossRef]

14. Lebek, B.; Uffen, J.; Breitner, M.H.; Neumann, M.; Hohler, B. Employees’ information security awareness and behavior: A literature review. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2013; pp. 2978–2987.

15. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* 1991, 50, 179–211. [CrossRef]

16. Häußinger, F. Studies on Employees’ Information Security Awareness. Ph.D. Thesis, Niedersächsische Staats-und Universitätsbibliothek Göttingen, Göttingen, Germany, 2015.

17. Kim, S.H.; Yang, K.H.; Park, S. An integrative behavioral model of information security policy compliance. *Sci. World J.* 2014, 47. [CrossRef] [PubMed]

18. Gibbs, J.P. Crime, punishment, and deterrence. *Southwest. Soc. Sci. Q.* 1968, 48, 515–530.

19. Rogers, R.W. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*; The Guilford Press: New York, NY, USA, 1983; pp. 153–176.

20. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 1989, 319–340. [CrossRef]

21. Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T.; Vance, A. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *Eur. J. Inf. Syst.* 2009, 18, 126–139. [CrossRef]

22. Taherdoost, H. A review of technology acceptance and adoption models and theories. *Procedia Manuf.* 2018, 22, 960–967. [CrossRef]

23. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* 2014, 37, 1049–1092. [CrossRef]

24. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* 2012, 31, 83–95. [CrossRef]
25. Brown, D.A. Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies. Ph.D. Thesis, Walden University, Walden, UK, 2017.

26. Weigel, F.K.; Hazen, B.T.; Cegielski, C.G.; Hall, D.J. Diffusion of innovations and the theory of planned behavior in information systems research: A metaanalysis. Commun. Assoc. Inf. Syst. 2014, 34, 31. [CrossRef]

27. Li, Y.J.; Hoffman, E. Information Security Policy Compliance. 2018. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3252742 (accessed on 25 May 2020).

28. Iriqat, Y.M.; Ahlan, A.R.; Molok, N.N.A. Information security policy perceived compliance among staff in palestine universities: An empirical pilot study. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Aveiro, Portugal, 9–11 April 2019; pp. 580–585.

29. Bauer, S.; Bernroider, E.W. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM Signis Database Database Adv. Inf. Syst. 2017, 48, 44–68. [CrossRef]

30. Guhr, N.; Lebek, B.; Breitner, M.H. The impact of leadership on employees’ intended information security behavior: An examination of the full-range leadership theory. Inf. Syst. J. 2019, 29, 340–362. [CrossRef]

31. Humaidi, N.; Balakrishnan, V. Indirect effect of management support on users’ compliance behavior towards information security policies. Health Inf. Manag. J. 2018, 47, 17–27.

32. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 2009, 47, 154–165. [CrossRef]

33. Ali, F.; Rasoolimanesh, S.M.; Cobanoglu, C. Applying Partial Least Squares in Tourism and Hospitality Research; Emerald Group Publishing: Bingley, UK, 2018.

34. Chin, W.W. Commentary: Issues and Opinion on Structural Equation Modeling; Management Information Systems Research Center, University of Minnesota: Minneapolis, MN, USA, 1998.

35. Ayatollahi, H.; Shagerdi, G. Information security risk assessment in hospitals. Open Med. Inform. J. 2017, 11, 37. [CrossRef]

36. Jalali, M.S.; Razak, S.; Gordon, W.; Perakslis, E.; Madnick, S. Health care and cybersecurity: Bibliometric analysis of the literature. J. Med. Internet Res. 2019, 21, e12644. [CrossRef]

37. Jarrett, M.P. Cybersecurity—A serious patient care concern. JAMA 2017, 318, 1319–1320. [CrossRef]

38. Rahman, R.; Alsharqi, O.Z. What drove the health system reforms in the Kingdom of Saudi Arabia? An analysis. Int. J. Health Plan. Manag. 2019, 34, 100–110. [CrossRef]

39. Chikhaoui, E.; Sarabdeen, J.; Parveen, R. Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia. Commun. IBIMA 2017, 2017, 1–18. [CrossRef]

40. Abraham, S. Information Security Behavior: Factors and Research Directions. AMCIS, 2011. Available online: https://aisel.aisnet.org/amcis2011_submissions/462 (accessed on 25 May 2020).

41. Klein, R.H.; Luciano, E.M. What influences information security behavior? A study with Brazilian users. J. Inf. Syst. Technol. Manag. 2016, 13, 479–496. [CrossRef]

42. Kurpis, L.V.; Beqiri, M.S.; Helgeson, J.G. The effects of commitment to moral self-improvement and religiosity on ethics of business students. J. Bus. Ethics 2008, 80, 447–463. [CrossRef]

43. Vance, A.; Siponen, M.; Pahnila, S. How Personality and Habit Affect Protection Motivation. In Proceedings of the Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP 2009), Phoenix, AZ, USA, 6–16 December 2009; pp. 1–7.

44. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User acceptance of information technology: Toward a unified view. MIS Q. 2003, 27, 425–478. [CrossRef]

45. Borena, B.; Bélanger, F. Religiosity and information security policy compliance. In Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, IL, USA, 15–18 August 2013.

46. Haeussinger, F. Understanding the antecedents of information security awareness-an empirical study. In Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, IL, USA, 15–17 August 2013.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).