The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses

Ke Dong 1,*, Rao Faizan Ali 2,*, P. D. D. Dominic 2 and Syed Emad Azhar Ali 3

Citation: Dong, K.; Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A. The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. Sustainability 2021, 13, 2800. https://doi.org/10.3390/su13052800

Abstract: The advancement of information communication technology in healthcare institutions has increased information security breaches. Scholars and industry practitioners have reported that most security breaches are due to negligence towards organizational information security policy compliance (ISPC) by healthcare employees such as nurses. There is, however, a lack of understanding of the factors that ensure ISPC among nurses, especially in developing countries such as Malaysia. This paper develops and examines a research framework that draws upon the factors of organizational climate of information security (OCIS) and social bond theory to enhance ISPC among nurses. A questionnaire was adopted in which responses were obtained from 241 nurses employed in 30 hospitals in Malaysia. The findings from the study demonstrated that the ISPC among nurses is enhanced through OCIS factors. The influence on ISPC was even more significant when examined by the mediating effect of the social bond. It implies that influential OCIS factors reinforce social bonds among nurses and eventually increase the ISPC. It implies that influential OCIS factors reinforce social bonds among nurses and eventually increase the ISPC. For information security practitioners, the study findings emphasize the prevalence of socio-active information security culture in healthcare organizations to enhance ISP compliance among nurses.

Keywords: security policy compliance; security breaches; organizational climate; social bond; healthcare information systems; multi-mediation; developing countries

1. Introduction

Information systems have become one of the most critical enablers of healthcare establishments in the information economy era due to their role in data management and smooth healthcare operations [1]. Unfortunately, information systems (IS) have become a target of choice for adversaries because their disruption can cause substantial financial and reputational losses [2,3]. Information security (Infosec) is a sub-branch of IS responsible for assuring confidentiality, integrity, and information systems availability [4,5]. Many technical and non-technical factors can cause infosec breaches. Studies have witnessed that infosec breaches result from non-technical factors such as employee negligence [6,7]. Therefore, the employee’s behavior should be controlled and restricted to ensure infosec compliance [8]. An essential instrument for ensuring infosec is an organization’s information security policy (ISP). An effective ISP is created in-line with international security standards and best practices [9]. ISP states an organization’s commitment to meet infosec standards by outlining employees’ expected and non-expected behavior. It also determines the penalties for violation of ISP [10]. However, ISP alone is not enough for ensuring the security of any organization. An organization must implement an effective information security policy compliance (ISPC) framework [11,12].
The issue of ISPC has been addressed by an organization and in studies through technical and non-technical solutions. Among the studies using advocating solutions, ref. [13] developed a fake online repository generation engine for cyber deception to solve behavioral infosec problems. Furthermore, ref. [14] presented a multimedia social network model for improving behavioral infosec among employees. Alongside, organizations are also required to develop non-technical solutions to enhance ISPC [15]. According to a report published by IBM, 95% of security breaches occur due to non-technical factors such as human negligence [16]. Parallel to this, literature has also argued that social bonding among employees is a determinant of ISPC [17,18]. A study by [19] concluded that employees are less vulnerable to negligence if they have better social bonding with work, colleagues, and family. Likewise, ref. [18] investigated employees’ behavior towards ISPC from the lens of socialization and cognition. His research proved commitment to ISP, attachment with organization, involvement in specific activities like infosec, and belief that protective behavior towards infosec is essential in safeguarding organizational infosec. In another study, ref. [20] investigated employees’ deviant infosec behaviors. The study results stated that individuals with adequate social bonding within the organizations have fewer chances to violate the ISP.

Researchers have shown a growing interest in creating an ISPC framework for organizations like those in the health sector [21]. Most of the studies were conducted in developed countries [11,22–24]. Simultaneously, only a few of those studies were conducted in the context of developing countries like Malaysia. Second, most of the designed frameworks for healthcare organizations lack a behavioral assessment of employees towards ISPC [25]. Furthermore, ref. [26] presented a qualitative study of healthcare employees’ perception of information governance policies.

Similarly, ref. [26] indicated that behavioral infosec controls in healthcare organizations should be investigated. Likewise, ref. [22] studied the infosec awareness and communications problem in the healthcare sector. They have provided several frameworks regarding infosec violations in healthcare institutions and showed that lack of compliance with the ISP is a severe issue. However, all the studies were examined in developed countries; therefore, their findings cannot be generalized to a developing country like Malaysia. Organizations’ infosec in developing countries is confronted with a much different climate, such as top management’s belief and control compared to developed countries [27–29]. As per the evaluation by [30] on the Malaysian healthcare sector regarding security culture and awareness, their results suggested a dire need to investigate the determinants of ISPC among Malaysian healthcare organizations. Accordingly, ref. [31,32] presented frameworks regarding ISPC in Malaysian healthcare organizations, but they have only tested the factors such as health belief model, working experience effects, and infosec awareness effects on ISPC. Furthermore, ref. [31,32] suggested that ISPC in healthcare organizations can be improved by factors of organization climate especially, top management support and socialization among healthcare employees.

Organizations’ management plays a vital role in strengthening climate-related to ISPC [28,33]. The organizational climate (OC) is defined in literature as a multi-dimensional construct that consists of multiple properties [11,28] and can affect the attitude of employees [34]. An effective organizational climate substantially affects employees’ motivation to enhance an organization’s policy compliance [35,36]. Existing literature explored that multiple OC factors such as top management beliefs and controls can significantly affect ISP compliance [11,28]. This study aims to advance the efforts of [31,32,37]. According to their research, there is a need to examine top management beliefs about IS security issues and administrative control over the IS security issues to enhance healthcare employees’ ISPC. This study only includes two OC factors: top management beliefs about IS security issues and organizations’ control of IS security issues. We have denoted these factors with the name of organizational climate information security (OCIS) factors. These factors have also been embarked on in literature in the context of infosec [28,38]. However, an empirical examination within the infosec context of a healthcare organization is still a research av-
venue yet to be explored, especially in a developing country like Malaysia. Furthermore, previous studies have not incorporated the effect, employees’ social bond can improve the ISPC, which according to [19,28,39] is one essential determinant of ISPC. To the best of our knowledge, few studies have investigated the effect employees’ social bond plays in explaining the change in ISPC, especially for healthcare organizations in developing countries like Malaysia.

We have selected Malaysia as a suitable research case for this study. Malaysian healthcare organizations lack a systematic theoretical and practical investigation of non-compliance’s adverse effects with ISPs [32,40]. Malaysian healthcare organizations have more advanced tools and techniques than most developing countries, but their behavioral infosec controls still need improvement [41]. The health information systems (HIS) have multiple components such as Financial Information System (FIS), Clinical Information System (CIS), Nursing Information System (NIS), Laboratory Information Systems (LIS), Picture Archiving Communication System (PACS), and Pharmacy Information System (PIS). Among these health information systems, it is challenging to ensure ISPC for users of NIS and CIS [42,43]. NIS and CIS’s use needs effective handling of private and sensitive information for patients that nurses primarily manage in healthcare organizations [44,45].

It is therefore essential that ISPC is ensured, especially among health care nurses. On the opposite, nurses are more hesitant to comply with ISPC [46,47].

In view of the scope, the current study aims to improve ISPC among nurses through OCIS factors and with the role of social bonding as a mediator. Centered on this context, this study discusses and answers the following research questions:

RQ1: Do the OCIS factors (i.e., top management beliefs about IS security issues and organization’s control of IS security issues) enhance social bonding among the nurses in healthcare organizations of developing countries?

RQ2: Does the adoption of social bond factors predict nurses’ behavioral intentions towards ISPC in developing countries?

The background of the research has been presented in Section 2. Formulation of the research framework and hypotheses are described in Section 3, while the research methodology is described in Section 4. A detailed results evaluation has been illustrated in Section 5—discussion and conclusions presented in Sections 6 and 7.

2. Background and Related Literature

Health information systems (HIS) has been introduced in Malaysia in the late 90s. Since then, different government and private hospitals have been utilizing HIS for various purposes [32]. HIS is a multipurpose system that holds records of patients, hospital management, and staff. HIS can be used as a web application or accessed from the internet for data updates and storage. Besides, ease of system accessibility can be vulnerable [31]. The data of HIS is susceptible, and it requires more security and protection. Appropriate security is needed for the personal health information of patients. Regardless of the nature of the information in healthcare environments, users do not take infosec seriously. Some employees have legitimate access to HIS, and negligence can harm the confidentiality of patients’ personal records [11,27].

Due to inadequate compliance with ISPs and employee knowledge, severe violations of data privacy have been reported. According to National surveys, many infosec breaches in the healthcare sector have occurred due to human factors such as lack of knowledge and ignoring infosec policies [48]. To achieve successful system information protection [30], health institutions need more commitment to monitoring these human-associated security breaches. It is noted that health organizations have experienced severe security breaches not only because of technical errors but also because of inefficient security culture, security knowledge, and security management among the organization’s employees [49]. According to a study published in the United Kingdom (UK) [50], technology-based errors account for five percent of a security breach than 95 percent, which was related to inefficient security knowledge employees. Some researchers find that deviant employee security conduct
is the biggest threat to healthcare organizations [4,31]. Simultaneously, limited data is available regarding the reason for such behavior in one such study [40]. They have stated that all individuals need to recognize the value of ensuring the protection of organizations. To enhance awareness, there is a dire need to create robust security awareness programs, explaining to the employees how to protect sensitive information’s confidentiality and integrity (i.e., patients’ health records) [51].

Table 1 presenting existing HIS behavioral infosec research findings and limitations. Most of the studies conducted in developed countries, such as [11], presented a study on 252 medical staff, including nurses from United States (US). They proved that majority of security incidents occur because of employees’ negligence. Similarly, ref. [22] conducted a US study with only 64 employees, including nurses, and stated that infosec awareness has no relation to the interval’s demographic profile. Furthermore, ref. [23] conducted a qualitative study in Swedish healthcare organizations and indicated that user intent rationalizations should not be measured through predefined behavior assumptions.

Table 1. Comparison with existing literature (limitations of existing studies).

| Authors | Sample Size | Country | Findings | Limitations |
|---------|-------------|---------|----------|-------------|
| [11]    | 252 medical staff | US | The root of significant security breaches in healthcare organizations is employee negligence. | 1. Study conducted in a developed country. |
| [27]    | 433 employees from KSA | | Self-efficacy and religion or self-morality are the best predictors of employees’ ISPC. | 1. Study only conducted in a single city. 2. Data were collected only from public hospitals. |
| [41]    | 454 healthcare employees (i.e., nurses, paramedical staff) | Malaysia | Management support has an indirect effect on employee’s compliance behaviors. | 1. Data collected only from public hospitals. 2. only two behavioral variables were examined. |
| [52]    | 263 HIS users | Iran | Self-efficacy and security competency are influential factors for enhancing infosec effectiveness. | 1. Measuring overall HIS security effectiveness 2. Research is not specific for ISPC. |
| [37]    | 454 healthcare employees | Malaysia | Effective leadership from top management can enhance infosec awareness among healthcare employees. | 1. Data collected only from public hospitals. 2. The study’s focus was solely on infosec awareness. |
| [22]    | 64 responses participated | US | There is no difference in perceptions about ISPs among multiple groups of healthcare employees. | 1. Study conducted in a developed country. 2. Sample size is too small. |
| [23]    | 24 semi-structured interviews conducted from medical staff | Sweden | User intent rationalizations should not be measured through predefined behavior assumptions. | 1. Study conducted in a developed country. 2. Small dataset. |
| [24]    | 2108 incidents reported from 117 organizations | UK | Healthcare organizations employee’s poor infosec practices cause most security breaches. | 1. Study conducted in a developed country. 2. Mostly discussed technical problems and solutions. |
| [31]    | 42 responses collected from hospital staff | Malaysia | Technology acceptance model and theory of planned behavior can be useful for healthcare employees | 1. Study conducted in only one hospital. 2. Sample size is too small. |
| [26]    | 8 IT managers from healthcare organization participated | UK | Top management should treat employees; equally, reward and recognition can encourage infosec behavior of an employee | 1. Study conducted in a developed country. 2. Sample size is small. |
Similarly, ref. [24] presented a mixed-method study in UK healthcare organizations. The study suggested that weak infosec practices by employees of healthcare organizations cause most security breaches. A recent study by [27] presented a framework based on eight behavioral theories constructs. They have taken nine influential variables and tested them with a survey of 433 employees. Their study concluded that among multiple infosec behavior factors, self-efficacy and religion or self-morality are the best predictors of employees’ ISPC. Similarly, ref. [26] examined HIS employees’ infosec behaviors and conducted a qualitative study. The analysis of the study indicated that top management support could enhance infosec behaviors of Healthcare employees.

Meanwhile, studies conducted in developing countries also have some useful findings and limitations. Reference [41] conducted quantitative research with 454 employees (i.e., nurses and paramedical staff) from Malaysian public hospitals and indicated that top management support could enhance healthcare employees’ self-efficacy and trust. The data was collected from the public hospitals; therefore, this study’s findings cannot be generalized to the whole sector. Similarly, ref. [52] examined self-efficacy and user competence towards the effectiveness of end-user HIS security. The study’s scope was very general and not specific towards ISPC in healthcare organizations. Similarly, ref. [31] have experimented with ISPC among Malaysian healthcare employees, including nurses, and stated that the technology acceptance model and the TPB could help assess employees’ security behavior. The study’s limitations were the data was only collected from one hospital, and only 42 employees participated.

The current study aims to advance [31,32,37,41] by addressing their limitations. As exhibited in Table 1, the studies conducted in developing countries have multiple limitations. Most of the studies are not measuring ISPC exactly but measuring other aspects of HIS infosec. Moreover, studies conducted in developing countries mostly experimented on the employees of public healthcare organizations. Thus, their findings cannot be generalized for ISPC in private healthcare organizations as both organization forms have variant organizational climate factors that develop their ISPC.

In contrast, we have developed a comprehensive research framework with the help of existing literature findings and limitations. However, fewer studies have highlighted ISP-related factors that cause the NIS and CIS security breaches in developing countries. However, few researchers have discussed the role of OCIS factors, social bonding, and ISPC, which leads to IS security breaches.

3. Research Framework and Hypothesis

Previous research showed that an individual’s attitude depends on community, friends, and family has perceived internal and external feelings. The employee’s attitude has a strong influence on complying with the ISP [18]. Several research models have been presented to illustrate the essential factors of ISPC [53–57]. Multiple research frameworks have predicted employees’ attitudes towards ISPC, but implementing these complex frameworks in an unpredicted environment, such as the healthcare sector, is nearly unattainable and non-feasible. A simple and effective research framework is required for accessing healthcare employees, especially for nurses. When a large enterprise is selected for ISPC, the first step is to comprehend OC (specifically top management concerns with IS security), enforcing the need for ISPC [28,38]. Multiple studies have indicated that effective OC can enhance an organization’s security culture [11,33,38].

3.1. Organizational Climate (OC)

OC is a multi-dimensional component that includes collecting properties that directly or indirectly affect employees’ attitudes [34]. The OC has substantially affected employees’ motivation to achieve the highest outcomes [35]. The OC’s dynamic nature includes multiple variables that have significant effects on employees’ attitudes. As described earlier, this study focuses on two OC factors: top management beliefs on IS security issues and the organization’s control of IS security issues. Each factor has its proven validity in
ISPC and has been used numerous times in the literature. For example, ref. [28,58] used top management beliefs on IS security issues and the organization’s control of IS security issues to investigate employees’ ISPC.

The fundamental explanation for considering these two OC constructs is that several studies have shown a lack of support from top management for IS security issues [30–32]. In the current study, we tried to determine how much top management support and organizational influence over IS-related issues would boost compliance with ISPs in health organizations. Furthermore, it has been shown in the previous literature that top management beliefs and organizational control over IS-related issues have a significant effect on individual’s attitudes [11,38]. Hence,

**Hypothesis 1a (H1a).** Top management beliefs about IS security issues have positive effects on nurses’ attitude towards ISPC.

**Hypothesis 2a (H2a).** Organizations control of IS security issues has positive effects on nurses’ attitude towards ISPC.

One study investigated attachment and OCIS factors relationship and stated that OCIS and attachment (i.e., social cohesion, communications, and so on) has a positive association [59]. Similarly, multiple researchers have confirmed OCIS’s supportive roles and individual attachment and satisfaction [60]. Thus,

**Hypothesis 1b (H1b).** Top management beliefs about IS security issues positively affect the nurses’ attachment towards organizational ISPs.

**Hypothesis 2b (H2b).** Organization’s control of IS security issues positively affects the nurses’ attachment towards organizational ISPs.

Literature showed that if an organization has good OC, employees tend to accept their organization’s rules and regulations. Moreover, good OC enhances individual bonds and linkages with other organization employees to facilitate organizational goals [59,61–63]. The study by [59] established that OCIS factors help maintain a sustainable relationship between employees and organizations. Thus,

**Hypothesis 1c (H1c).** Top management beliefs about IS security issues positively affect the nurses’ commitment towards organizational ISPs.

**Hypothesis 2c (H2c).** Organization’s control of IS security issues positively affects the nurses’ commitment towards organizational ISPs.

Reference [61] proved that supportive OC factors significantly predict an individual’s involvement with their organization’s objectives. Likewise, ref. [62] have surveyed 1413 employees of 42 countries and found a significant relationship between individual involvement and OC. It is expected that a helpful climate reinforces individuals’ involvement in their organization’s objectives. Thus,

**Hypothesis 1d (H1d).** Top management beliefs about IS security issues positively affect the nurses’ involvement towards organizational ISPs.

**Hypothesis 2d (H2d).** Organization’s control of IS security issues positively affects the nurses’ involvement towards organizational ISPs.

The relationship between personal norms and social behaviors has long been recognized in literature [64]. Previous research has shown that OCIS factors and personal norms are positively associated [28]. Similarly, ref. [65,66] examined organizational norms’ influ-
ence on IS security issues and stated that IS security issues significantly affect individual’s personal norms. Hence,

**Hypothesis 1e (H1e).** Top management beliefs about IS security issues positively affect nurses’ personal norms towards organizational ISPs.

**Hypothesis 2e (H2e).** Organization’s control of IS security issues positively affects nurses’ personal norms towards organizational ISPs.

### 3.2. Social Bond Theory (SBT)

Travis Hirschi initially proposed the social bond theory in 1969 [67] that later arose as social control theory. The social bond theory is an exciting way to reaching out to the social problems of individuals. The social bond theory by [67] encapsulates an employees’ attachment to families, commitment to social norms and institutions (i.e., school and employment), involvement in activities, and the belief that these things are important” [68]. The social bond theory is derived from the General Theory of Crime; according to social bond, crime happens when a person’s social bond is weak. This theory describes the social values and social relations between individuals, their social values and their perception of something, their attachment to peers, their participation in their work, their dedication to their goals, and their belief in society’s shared values [19,69]. The social bond theory has four main components—attachment, commitment, involvement, and personal norms [67]. There are plenty of research studies that have tested social bond theory in the context of ISP’s compliance and have deduced that an employee’s compliance with policies is a function of his/her attachment towards the organization [18,19,28].

Reference [67] noted that it might deter antisocial behavior when a person forms an attachment to others. It has been shown that these attachments appear to make them collectively more agreeable to maintaining principles essential to their organizations when co-workers build close bonds with peers [70,71]. IS security researchers found that employees who socialize with peers concerning IS security concerns appeared to be more compliant with IS security regulations [10,18,33,72].

**Hypothesis 3 (H3).** Attachment with organizational security issues will positively influence attitude towards the ISPC.

The commitment to a social group or association encourages a sense of social accountability and honors, according to [67]. Employees’ commitment to an organization plays an essential role in promoting or discouraging IS security behaviors [18]. Thus, if their commitment to the organization is strong, an employee is less likely to participate in counterproductive IS behaviors that can undermine their organization’s IS resources [19,58].

**Hypothesis 4 (H4).** Commitment to organizational security issues will positively influence attitude towards the ISPC.

Reference [67] believed that psychological development was incompatible with isolation. It is expected that an employee’s involvement in the issues of their company, including IS security issues, would gain some gratification from such an exercise. In general, organizations’ long-term performance bodes well for such involvement, commitment, and personal relationships with colleagues [33]. Studies by [18,73] using the same measuring items comparable to this study showed that the involvement of employees in the IS security problems of their organizations positively influenced attitude to comply with the organizational policies [19,28]. Hence,

**Hypothesis 5 (H5).** Involvement with organizational security issues will positively influence attitude towards the ISPC.
Various IS researchers have proposed that the employees’ interpretation of organizational issues is essential to personal norms and individual values. It also includes compliance with appropriate computer conduct and security guidelines [72–74]. Therefore, supporting the relationship between compliance with IS security personal norms and ISPC [19,28]. Their findings showed that employees with favorable IS security personal norms were more likely to comply with their organizations’ IS rules [15,19,28,39,75]. Thus, Hypothesis 6 (H6). *Employees’ personal norms positively influence attitude towards the ISPC.*

3.3. Attitude

Attitude is defined as the individual’s positive or negative feelings toward engaging in a specified behavior [18]. This research study captures attitude towards ISPC. Hence, Hypothesis 7 (H7). *Nurses’ attitudes towards organizational policies will positively influence intention towards the ISPC.*

Based on our research hypotheses, Figure 1 below exhibits the research framework of this study. Whereas, Figure 2 demonstrates the multi-mediation model of this study.
4. Research Methodology

This study follows the quantitative research design. The descriptive analysis is integrated with five-point Likert scales ranging from strongly disagree to strongly agreed. The quantitative research method [67] was chosen based on the adopted constructs' confirmation and generalization. Quantitative research design determines the theory using statistical analysis. Besides, Table 2 provides a comparison of various study designs. The "Quantitative" column of Table 2 highlights the main features of quantitative research in line with this study's scope.

4.1. Pilot Test

To validate and improve our research instrument (i.e., questionnaire), we performed a pilot study to evaluate scale items' reliability and validity. The developed questionnaire was distributed to four public and private hospitals in Malaysia to collect quantitative analysis data. Emails were sent to nurses, and a total of 61 responses were gathered. From the 61 responses, the number of female respondents was higher than that of male respondents. Both private and public hospital nurses reacted appropriately. Furthermore, daily computer usage was documented, which indicates that nurses from different backgrounds and divisions participated. The everyday computer use was recorded from 4 h to 12 h. Most of the respondents know that their organizations have information protection procedures and policies, but most of them do not have the deep knowledge about their organizational ISPs.

| Variable                  | Quantitative          | Qualitative                  | Mixed-Method               |
|---------------------------|-----------------------|------------------------------|----------------------------|
| Sample size               | Large                 | Small                        | Mix: small and large       |
| Data type                 | Numerical data        | Textual raw data             | Both type of data          |
| Relationship with         | No direct relationship.| Close-one-to-one relationship.| Both type of relationship  |
| participants              |                       |                              |                            |
| Generalizability          | Highly generalizable  | Generalizability is not an   | Generalizability is more    |
|                           |                       | objective                    | robust than the other       |
|                           |                       |                              | two methods                 |
| Results interpretation    | Concise interpretation of results due to use of statistics | Many Interpretations | Interpretation is complicated because of the use of both methods |
| Overall aim               | Generalization and confirmation | Explanation and understanding of social phenomena | Both explanation and generalization |

4.2. Sampling Procedure

This study aims to collect data of CIS and NIS users (i.e., doctors and nurses). However, the doctors' data collection was challenging because of doctors' busy schedules and COVID-19 routine; therefore, we decided to collect nurses' data. Second, nurses' use of CIS and NIS is more than any other hospital staff (i.e., doctors and surgeons) [43,47]. According to a report published by Arch Collaborative, nurses have a longer HIS usage training period than doctors. Furthermore, the report identified that nurses are more frequent HIS users than physicians and other hospital staff [76]. Therefore, the nurses working in public and private hospitals in Malaysia were the sample population for this study.

Information relating to nursing workers was extracted from the Report 2000–2020 of Malaysia's Health Ministry [77]. As per the report, 106,289 nurses are working in public and private hospitals. It was impossible to get a full list of all the nurses. Therefore, we extracted the sample population from the [78] predefined table to generalize the findings.

We collected data from the four Malaysian states: Kuala Lumpur, Selangor, Johor, and Perak. It was near too impossible to approach all the nurses working in all the hospitals. Therefore, hospitals were chosen with the simple random sampling (SRS) method.
SRS, we selected a total of 30 hospitals out of 120 and approached them for data collection. We concentrate on those departments that often deal with humans and computers.

It was impossible to approach all nurses in 30 hospitals because of the resources and time limitations. Therefore, the second round of simple random sampling (SRS) was carried out with each hospital’s HR department’s aid. Finally, randomly selected nurses from each hospital department contribute to this study. We collected the data using self-administered questionnaires by sending google forms to HR departments’ email addresses.

To validate the results, we use Partial Least Square-based Structural Equation Modelling (PLS-SEM) technique. For data analysis, the data range between 200–400 is adequate [79]. We submitted questionnaires to 300 nurses and collected a total of 250 responses. Two hundred forty-one correct responses were taken for further review after the process of data screening. For primary statistical analysis, SPSS-23 was employed. Whereas Smart PLS 3 was used for performing the SEM techniques.

4.3. Measurement Items

The survey was conducted using a simple random sampling technique of Malaysian public and private hospitals. In this perspective, a questionnaire was adapted and measured on a five-point Likert scale ranging from “1 = strongly disagree” to “5 = strongly agree”.

Organizational climate has two sub-constructs; top management beliefs about IS security issues and organization’s control of IS security issues. Top management beliefs about IS security issues were measured using four items adapted from [28]. The organization’s control of IS security issues was measured by three items adapted from [28]. The attachment was measured with four items adapted from [19], a commitment was measured with four items adapted from [19,80]. Whereas involvement was measured by four items adapted from [80], and personal norms were measured with four items adapted from [15,80]. The attitude was measured by four items and adopted from [15]. Finally, the ISPC was measured with four items adapted from [15,18].

5. Data Analysis and Results

In this research, the data were gathered from survey instruments. We first performed a descriptive analysis test followed by demographic analysis. After these, the researcher executed the construct, convergent, and discriminant validity tests. Finally, we tested the hypotheses.

5.1. Descriptive Analysis

Table 3 demonstrates the descriptive values of the constructs. The mean values of all constructs are positive. All the participants of this research study responded positively to OC’s top management beliefs about IS security issues (i.e., Top Management Beliefs-TMB) and the organization’s control of IS security issues (OCS). The social bond, manifested by Attachment (ATC), Commitment (COM), Involvement (INV) and Personal Norms (PN). At the same time, ISPC demonstrates the intention to security policy compliance. Lastly, ATT represents the attitude to comply with ISP. Typically, the symmetry of data is defined by skewness. The values of all the 0 are negatively skewed.

Table 4 demonstrates the demographic statistics utilized in this study. Data analysis indicated that most of the respondents are between 25 to 35 of age, with 38%. Most nurses process an undergraduate degree with 63% and preferably from the public organizations (66%). Results also indicated that nurses with one to five years of experience are more participative than other age groups. Furthermore, they are aware of the security policy (76%) and information technology competence at a high rate (52%).
Table 3. Descriptive Analysis Results.

| Constructs | Mean   | Standard Deviation | Excess Kurtosis | Skewness |
|------------|--------|--------------------|-----------------|----------|
| TMB        | 3.724  | 0.920              | −0.624          | −0.54    |
| OCS        | 3.956  | 0.905              | −0.702          | −0.302   |
| ATC        | 4.213  | 0.818              | 3.777           | −1.709   |
| COM        | 4.045  | 0.891              | 1.545           | −1.249   |
| INV        | 4.038  | 0.883              | 1.577           | −1.189   |
| PN         | 3.652  | 0.903              | −0.247          | −0.372   |
| ATT        | 3.835  | 0.972              | 0.353           | −0.977   |
| ISPC       | 3.769  | 0.976              | −0.179          | −0.594   |

Table 4. Demography of Dataset.

| Demographic Variable | Categories | Frequency (n = 241) | Percentage (%) |
|----------------------|------------|---------------------|----------------|
| Age (range in years) | 25–35      | 98                  | 38             |
|                      | 35–45      | 73                  | 30             |
|                      | 45–55      | 45                  | 18             |
|                      | 55–65      | 25                  | 10             |
| Education            | Undergraduate | 152                | 63             |
|                      | Graduate    | 89                  | 36             |
| Sector               | Public      | 160                 | 66             |
|                      | Private     | 81                  | 34             |
| Experience           | 1–5         | 131                 | 54             |
|                      | 6–15        | 70                  | 29             |
|                      | 16–25       | 25                  | 10             |
|                      | 26–35       | 15                  | 06             |
| Information Technology| Low        | 115                 | 47             |
|                      | High        | 126                 | 52             |
| Daily usage of computers (hours) | 4–7 | 87 | 36 |
|                      | 8–11        | 139                 | 57             |
|                      | More than 11| 15                  | 06             |
| Existence of ISPs    | Yes         | 209                 | 86             |
|                      | No          | 20                  | 08             |
|                      | I Don’t know| 12                  | 04             |
| Awareness of ISPs    | Not aware   | 13                  | 05             |
|                      | Somewhat aware | 45              | 19             |
|                      | Very much aware | 183            | 76             |

5.2. Assessment of Measurement Model

We assess the measurement model through Smart PLS. Furthermore, the assessment of measurement model was evaluated through convergent validity and discriminant validity.

5.2.1. Convergent Validity

The measurement model was evaluated in terms of reliability, the validity of the constructs, and factor loadings. Table 5 represents all the convergent validity values. The threshold values for factor loadings are 0.5-factor; the loading value must not be less than 0.5. according to [81], one or two values less than 0.708 are acceptable. For reliability and validity, we have used Cronbach’s alpha coefficient, which shows the consistency between the items; according to [82], Cronbach’s alpha value should not be less than 0.70. in this contrast, composite reliability is determined based on factor loadings, and it should be greater than 0.70 [83]. Meanwhile, the average variance extracted (AVE) value for each construct should not be less than 0.05, reflecting the construct’s appropriateness.
The values of rho_A and Chronbach’s alpha were above 0.7 for each construct stipulated that items are reliable for measurement. Furthermore, all constructs’ AVE and CR values are more significant than 0.5, which indicated sufficient convergent validity [84].

Table 5. Convergent validity.

| Constructs | Items                                                                 | Loadings |
|------------|-----------------------------------------------------------------------|----------|
| Organizational Climate                                                                                                                                  |
| Top management believes about IS security issues                                                | TMB1 0.788 |
| Management is worried about employee participation in IS security issues                        | TMB2 0.781 |
| The management of my organization deals with information security issues effectively.       | TMB3 0.881 |
| Top management believes that the IS security policy of the company offers valuable business advantages to the firm. | TMB4 0.769 |
| Organization’s control of IS security issues                                                   | OCS1 0.771 |
| My organization organizes information security discussions                                     | OCS2 0.781 |
| My organization effectively plans and monitors the processes and procedures for information security. | OCS2 0.781 |
| My company sufficiently coordinates its policies and procedures on information security.     | OCS3 0.881 |
| Social Bond Theory                                                                                                                                   |
| Attachment                                                                                                                                       |
| The concerns of my organization about information security incidents are important to me     | ATC1 0.774 |
| I would like to communicate with my colleagues on the importance of organizational information security policies. | ATC2 0.778 |
| The opinions and views of my peers on organizational, informational policies are important to me. | ATC3 0.662 |
| I always pursue information security policies to ensure that my organization has a safe atmosphere. | ATC4 0.881 |
| I usually have conversations about my organization’s information security policies with close co-workers | ATC5 0.802 |
| Commitment                                                                                                                                       |
| I strongly believe that information security policies will play a crucial role in my organizations’ success | COM1 0.774 |
| I am committed to promoting information security policy practices in my organization.       | COM2 0.785 |
| I will do my utmost to put my time and resources into the success of information security policies. | COM3 0.702 |
| I will put my all energies and resources to make my organization successful                  | COM4 0.751 |
| I always keep myself updated based on new organizational information security policies.    | COM5 0.700 |
| Involvement                                                                                                                                       |
| I appreciate the ability to take part in informal meetings important to my organization’s information security. | INV1 0.744 |
| To address information security policy issues, I work with several colleagues to develop personal relationships. | INV2 0.788 |
| I actively participate in events related to the growth of my organization.                  | INV3 0.703 |
| I feel that it is fair to cooperate with the information security team                      | INV4 0.714 |
Table 5. Cont.

| Constructs                          | Items                           | Loadings | Reliability       |
|-------------------------------------|---------------------------------|----------|-------------------|
|                                     |                                 | Cronbach’s Alpha | rho_A             |
| **Personal Norms**                  |                                 |           |                   |
| It’s critical if I don’t follow the organization’s ISP is unacceptable... | PN1    | 0.706               |                   |
| Not following all the rules and regulations outlined in the organization’s ISP is unacceptable... | PN2    | 0.701               | 0.770 0.771       |
| To me, it is not a trivial offense to obey the organization’s ISP | PN3    | 0.699               |                   |
| It is inappropriate for me to violate my company’s ISP. | PN4    | 0.788               |                   |
| **Attitude**                        |                                 | Cronbach’s Alpha | rho_A             |
| Following the organization’s ISP is a good idea | ATT1   | 0.778               |                   |
| Following the organization’s ISP is a necessity | ATT2   | 0.851               | 0.841 0.842       |
| Following the organization’s ISP is beneficial | ATT3   | 0.855               |                   |
| Following the organization’s ISP is pleasant | ATT4   | 0.741               |                   |
| **Intention towards Security Policy Compliance** |                                 |           |                   |
| It is my intention to continue to comply with the organization’s ISP | ISPC1  | 0.778               |                   |
| I am confident that I will stick to the ISP of my company. | ISPC2  | 0.889               | 0.831 0.832       |
| I am likely to follow the organization’s ISP in the future | ISPC3  | 0.881               |                   |
| I would follow the organization’s security policy whenever possible | ISPC4  | 0.885               |                   |

5.2.2. Discriminant Validity

Discriminant validity shows the statistical and theoretical variations of each pair of constructs involved in the study [83]. An accurate evaluation is critical as each construct should capture a phenomenon uniquely from the empirical aspects [84]. There are two frequently used methods to test discriminant validity, namely the Fornell-Larcker criterion and heterotrait-monotrait ratio of correlation (HTMT). HTMT is more reliable, unlike the other criterion [83]. The HTMT value is considered to be acceptable at <0.85 [83]. The HTMT value of all constructs is less than 0.85, as seen in Table 6.

The structural model evaluation was carried out in two non-exclusive ways: model fit and approximate model fit. The model fit test relies on geodesic discrepancy (dG) and unweighted least square discrepancy (dULS). At the same time, the standardized root means unbiased residuals (SRMR) and Normed Fit Index (NFI) is used in the estimated model fit test (NFI). As shown in Table 7, the value of SRMR below 0.08 [85] and the value of NFI above 0.9 is considered acceptable [86]. However, for strictly confirmatory studies, goodness-of-fit is theoretically useful.

Moreover, the absolute implementation of any measure of fit is still not fully developed [84]. The exact fit measurements d_ULS value did not meet the threshold for our model. As described by [87], there is little knowledge available on accurate fit measures. Their real usefulness, behavior, and relevance are not sufficiently represented in PLS literature thus far. Further, they have stated that PLS-SEM is primarily built on nonparametric evaluation criteria; therefore, exact fit measures used in covariance-based SEM are not universally transferable to PLS-SEM.

5.3. Assessment of Structural Model

5.3.1. Structured Model without Mediators

The relationship between exogenous (TMB and OCS) and endogenous variables (ATT & ISPC) were evaluated. The association between TMB and ATT is positive and significant (Path C: H1a: b = 0.645, t-value = 9.308, p < 0.05). Moreover, the relationship between OCS and ATT was also positive and significant (Path C: H2a: b = 0.332, t-value = 4.589, p < 0.05). The relationship between ATT and ISPC was positive and significant (H1a: b = 0.798, t-value = 16.217, p < 0.05). The direct effect TMB -> ATT and OCS -> ATT were significant.
Therefore, the direct effects were significant when the mediating variables were excluded from the PLS path model [81,88].

Table 6. Discriminant validity.

| Latent Construct | CR   | AVE  | (1)  | (2)  | (3)  | (4)  | (5)  | (6)  | (7)  | (8)  |
|------------------|------|------|------|------|------|------|------|------|------|------|
| TMB (1)          | 0.913| 0.692|      |      |      |      |      |      |      |      |
| OCS (2)          | 0.912| 0.730| 0.601|      |      |      |      |      |      |      |
| ATC (3)          | 0.917| 0.672| 0.547| 0.606|      |      |      |      |      |      |
| COM (4)          | 0.915| 0.676| 0.529| 0.534| 0.673|      |      |      |      |      |
| INV (5)          | 0.802| 0.714| 0.531| 0.601| 0.518| 0.511|      |      |      |      |
| PN (6)           | 0.832| 0.591| 0.630| 0.511| 0.509| 0.636| 0.566|      |      |      |
| ATT (7)          | 0.912| 0.701| 0.632| 0.611| 0.555| 0.512| 0.531| 0.521|      |      |
| ISPC (8)         | 0.887| 0.707| 0.607| 0.542| 0.533| 0.598| 0.518| 0.594| 0.511|      |

Black color: globally known format to report Discriminant Validity (HTMT).

Table 7. Model Fit Measures.

| Model Fit Measures | Acceptable Fit Indices | Obtained Indices |
|--------------------|------------------------|------------------|
| SRMR               | <0.08                  | 0.069            |
| NFI                | >0.9                   | 0.903            |
| d_ULS              | <0.95                  | 0.972            |
| d_G                | <0.95                  | 0.940            |

5.3.2. Structured Model with Mediators

The indirect or mediating effects of TMB & OCS constructs on ATT via social bond theory (ATC, COM, INV and PN) were examined through PLS-SEM technique recommended by [79,88,89]. The relationships among the concerned constructs were evaluated by bootstrapping (5000 resamples) [81] to generate the direct effect, confidence intervals, t-values and effect size ($f^2$) as shown in Table 7. By adding the mediating constructs, the direct association TMB → ATT (Path C') and OCS → ATT (Path C') were positive but not significant. According to Hair et al. (2014), the indirect effect a x b must be significant to established mediation effect. Table 7 showed that the association between top management beliefs about IS issues has a positive and significant predictor of commitment (COM) ($H_{1c}$: $b = 0.579$, t-value = 6.311, $p < 0.05$), TMB towards involvement (INV) ($H_{1d}$: $b = 0.655$, t-value = 8.242, $p < 0.05$) and TMB to personal norms (PN) ($H_{1e}$: $b = 0.558$, t-value = 7.140, $p < 0.05$). Moreover, organization’s control on IS security issues (OCS) has positively and significant association with COM ($H_{2c}$: $b = 0.571$, t-value = 8.072, $p < 0.05$), OCS towards personal norms (PN) ($H_{2e}$: $b = 0.292$, t-value = 5.376, $p < 0.05$). Finally, COM positively and significantly affect ATT ($H_{4}$: $b = 0.255$, t-value = 1.744, $p < 0.05$), INV significantly and positively affect ATT ($H_{5}$: $b = 0.227$, t-value = 1.508, $p < 0.05$), PN positively and significantly affect ATT ($H_{6}$: $b = 0.227$, t-value = 1.508, $p < 0.05$) and ATT positively and significantly affect ISPC ($H_{7}$: $b = 0.498$, t-value = 5.115, $p < 0.05$). Hence, the hypotheses $H_{1C}$, $H_{1d}$, $H_{1e}$, $H_{2C}$, $H_{2e}$, $H_{4}$, $H_{5}$, $H_{6}$ and $H_{7}$ were supported.

Additionally, we also report the $f^2$ effect size to check when a specified exogenous variable from the model is omitted. The omitted variable has a substantive effect on the endogenous variable [81]. The threshold value of $f^2$ is 0.02 (small), 0.15 (medium) and 0.35(large) effect of exogenous latent constructs [90]. Table 8 showed that all the supported constructs have a large effect on exogenous latent variables.
Table 8. Structured model and effect size.

| Relation | Direct Effect | t-Value | $f^2$ |
|----------|---------------|---------|-------|
| H1a TMB → ATT | 0.559 NSig | 3.204 | 0.14 |
| H1b TMB → ATC | 0.398 NSig | 4.568 | 0.03 |
| H1c TMB → INV | 0.579 Sig | 6.311 | 0.40 |
| H1d TMB → COM | 0.655 Sig | 8.242 | 0.70 |
| H1e TMB → PN | 0.558 Sig | 7.140 | 0.60 |
| H2a OCS → ATT | 0.21 N Sig | 0.396 | 0.02 |
| H2b OCS → ATC | 0.538 N Sig | 6.486 | 0.02 |
| H2c OCS → COM | 0.517 Sig | 8.072 | 0.60 |
| H2d OCS → INV | 0.252 N Sig | 1.689 | 0.05 |
| H2e OCS → PN | 0.292 Sig | 5.376 | 0.34 |
| H3 ATC → ATT | 0.137 N Sig | 1.414 | 0.03 |
| H4 COM → ATT | 0.255 Sig | 1.744 | 0.05 |
| H5 INV → ATT | 0.227 Sig | 1.508 | 0.02 |
| H6 PN → ATT | 0.368 Sig | 3.858 | 0.24 |
| H7 ATT → ISPC | 0.498 Sig | 5.115 | 0.55 |

5.4. Predictive Relevance

According to [81] stated that the values of $Q^2$ affirmed the accuracy and predictive relevance of the model. The values of $Q^2$ were calculated by using the blindfolding method in PLS-SEM. This technique effectively and accurately exhibits the data points of indicators in reflective models. In the structural model, $Q^2 > 0$ indicated that certain endogenous constructs indicate the path model predictive relevance of particular exogenous variables [88]. The threshold values of $Q^2$ is 0.02, 0.15 and 0.35 were referred to as weak, medium and robust effect respectively [81]. The $Q^2$ values of all endogenous variables were above 0.35 except ATC. It demonstrates an acceptable level of predicative relevancy of the model (Table 9).

Additionally, Table 8 showed the coefficient of determination ($R^2$), representing how an exogenous construct explains the endogenous construct’s relationship. The values of $R^2$ is 0.25 (weak), 0.50 (moderate) and 0.75 (strong) [81]. In the path model, the values of $R^2$ were relatively moderate and substantial expect ATC ($R^2 = 0.258$) (Table 9).

Table 9. Predictive relevance and coefficient of determination ($R^2$).

| Endogenous Variables | $Q^2$ | $R^2$ | Exogenous Variables |
|----------------------|-------|-------|---------------------|
| ATC                  | 0.206 | 0.258 | TMB, OCS            |
| COM                  | 0.637 | 0.678 | TMB, OCS            |
| INV                  | 0.660 | 0.724 | TMB, OCS            |
| PN                   | 0.584 | 0.581 | TMB, OCS            |
| ATT                  | 0.736 | 0.608 | TMB, OCS, ATC, COM, INV, PN |
| ISPC                 | 0.502 | 0.635 | ATT                 |

5.5. Multiple Mediating Effect Tests

To test the mediating role of attachment (ATC), commitment (COM), involvement (INV), and personal norms (PN) towards attitude (ATT), we applied the relatively new analytical method recommended by recent research studies [81,88,89]. Table 9 depicted the outcomes of direct, indirect, and total effects of the exogenous construct (TMB) on the endogenous construct (ATT) through their mediators (ATC, COM, INV, and PN). Moreover, the outcomes of multiple mediation paths along-with computation of their strengths and magnitude effects are also displayed in Figures 3 and 4 for a better illustration. The bootstrapping technique using bias-corrected and percentiles were applied to test the specific indirect effects.

In Table 10, the direct effect of TMB on ATT was positive but not significant (H1a: C‘I). Additionally, the outcomes revealed that the exogenous construct’s indirect effects were also
not significantly supported as 0 value was counted in 90% CI. The significance of structural coefficients was also checked by bias-corrected CI [89]. From Table 9, the path-a (a2, a3, and a4) was multiplied with path-b (b2, b3, and b4) to calculate the total indirect effect. The path-a of COM, INV, and PN were significant, but ATC’s path-a was not significant. Therefore, the H1b was rejected, and H1c, H1d, and H1e were accepted. Furthermore, ref. [81] recommended that mediation’s magnitude or strength is important in the complex structure path model. It can be measured by incorporating the variance accounted for (VAF) method. The value of VAF < 0.2 (no mediation); 0.2 ≤ VAF ≤ 0.8 is consider partial mediation and the value of VAF < 0.8 indicate full mediation (Hair et al., 2017). Table 9 and Figure 3 illustrates the magnitude of mediation in term of COM (a2b2), INV (a3b3) and PN (a4b4) mediate the relationship between TMB and ATT. As depicted in Table 10 and Figure 3, the VAF values under 0.2 ≤ VAF ≤ 0.8 indicate partial mediation [81], so the mediation hypotheses H1c, H1d, and H1e were supported.

Table 10. Summary of mediation effect of TMC on ATT through social bond theory constructs.

| Direct Effect | Coefficient | Bootstrap 90% CI | BC |
|---------------|-------------|----------------|----|
|               |             | Percentile     |     |     |
|               |             | Lower (5%)     | Upper (95%) | Lower (5%) | Upper (95%) |
| C'            | 0.559 Sig   | −0.111         | 0.376 | −0.264 | 0.529 |
| a2            | 0.579 Sig   | 0.319          | 0.545 | 0.315  | 0.541 |
| a3            | 0.655 Sig   | 0.429          | 0.64  | 0.422  | 0.633 |
| a4            | 0.558 Sig   | 0.429          | 0.687 | 0.425  | 0.683 |
| b2            | 0.255 Sig   | 0.025          | 0.305 | 0.021  | 0.301 |
| b3            | 0.227 Sig   | 0.016          | 0.259 | 0.014  | 0.261 |
| b4            | 0.368 Sig   | 0.189          | 0.497 | 0.209  | 0.517 |

| Indirect Effect | Point estimate | Percentile     |         |         |         | VAF |
|-----------------|----------------|----------------|---------|---------|---------|-----|
|                 |                | Lower (5%)     | Upper (95%) | Lower (5%) | Upper (95%) |
| a2 × b2         | 0.148 Sig      | 0.010          | 0.147   | 0.005   | 0.143   | 21% |
| a3 × b3         | 0.149 Sig      | 0.008          | 0.148   | 0.009   | 0.147   | 21% |
| a4 × b4         | 0.205 Sig      | 0.094          | 0.304   | 0.102   | 0.313   | 27% |
| Total Indirect effect | 0.434    | 0.111          | 0.600   | 0.116   | 0.602   | 69% |

Figure 3. Magnitudes of mediation paths TMB → ATT.
From Table 11, the direct effect of OCS on ATT was positive but not significant (H$_{2a}$: C'). Additionally, the outcomes revealed that the exogenous construct’s indirect effects were also not significantly supported as 0 value was counted in 90% CI. The significance of structural coefficients was also checked by bias-corrected CI [89]. Table 11, the path-a (i.e., a$_2$ and a$_4$) was multiplied with path-b (b$_2$ and b$_4$) to calculate the total indirect effect. The path-a of COM and PN were significant, but ATC and INV’s path-a were not significant. Therefore, H$_{2b}$ and H$_{2d}$ were rejected, and H$_{1c}$ and H$_{1e}$ were accepted. Furthermore, ref. [81] recommended that mediation’s magnitude or strength is important in the complex structure path model. It can be measured by incorporating the variance accounted for (VAF) method. The value of VAF < 0.2 (no mediation); 0.2 ≤ VAF ≤ 0.8 is consider partial mediation and the value of VAF < 0.8 indicate full mediation (Hair et al., 2017). Table 11 and Figure 4 illustrate the magnitude of mediation in terms of COM (a$_2$b$_2$) and PN (a$_4$b$_4$) mediate the relationship between OCS and ATT. As depicted from Table 11 and Figure 4, the VAF values under 0.2 ≤ VAF ≤ 0.8 indicate partial mediation [81], so the mediation hypotheses H$_{1c}$ and H$_{1e}$ were supported.

### Table 11. Summary of mediation effect of OCS on ATT through social bond theory constructs.

| Direct Effect | Coefficient | Bootstrap 90% CI | BC |
|---------------|-------------|-----------------|----|
|               |             | Percentile      | BC |
|               |             | Lower (5%)      | Upper (95%) | Lower (5%) | Upper (95%) |
| C'            | 0.21 $^\text{NSig}$ | $-0.098$ | $0.083$ | $-0.108$ | $0.073$ |
| a$_2$         | 0.517 $^\text{Sig}$ | 0.408 | 0.618 | 0.411 | 0.621 |
| a$_4$         | 0.292 $^\text{Sig}$ | 0.268 | 0.510 | 0.271 | 0.513 |
| b$_2$         | 0.255 $^\text{Sig}$ | 0.025 | 0.305 | 0.021 | 0.301 |
| b$_4$         | 0.368 $^\text{Sig}$ | 0.189 | 0.497 | 0.209 | 0.517 |

| Indirect Effect | Point estimate | Percentile      | BC | VAF |
|-----------------|----------------|-----------------|----|-----|
|                 |                | Percentile      | BC |     |
|                 |                | Lower (5%)      | Upper (95%) | Lower (5%) | Upper (95%) |     |
| a$_2$ × b$_2$   | 0.132 $^\text{Sig}$ | 0.013 | 0.154 | 0.013 | 0.153 | 39%  |
| a$_4$ × b$_4$   | 0.107 $^\text{Sig}$ | 0.071 | 0.203 | 0.082 | 0.214 | 34%  |
| Total Indirect effect | 0.239          | 0.084 | 0.357 | 0.095 | 0.367 | 72%  |

Figure 4. Magnitudes of mediation paths OCS → ATT.
5.6. Common Method Bias

We evaluated the threat of standard methods bias by taking steps to assure the respondents that their responses would be kept anonymous [91]. The standard method bias was evaluated via “the occurrence of VIF.” The threshold value of VIF greater or equal to 3.3 is indicated the data was collected from a single source; therefore, we investigate the threat of standard method bias by following the suggestions from [91,92]. We executed the collinearity test in SmartPLS. Table 12 depicted the full collinearity test and found that all the values are less than 3.3. These outcomes depicted that single source biasedness is not a severe problem in our data.

Table 12. Full Collinearity Test Results.

| TMB | OCS | ATC | COM | INV | PN | ATT | ISPC |
|-----|-----|-----|-----|-----|----|-----|------|
| 0.197 | 0.235 | 0.188 | 0.223 | 0.187 | 0.228 | 0.203 | 0.119 |

6. Discussion

Information security policy noncompliance in the health sector is a severe and neglected problem in today’s world [1]. This study contributes theoretically and practically to enhance understanding of ISPC in the health sector. OCIS factors such as TMB and OCS provided vital sources of security governance in the health sector. Consequently, this study contributes to the theory with OCIS and social bond factors, which have never been tested and analyzed in the healthcare sector. Furthermore, the current study implied that the provided framework is an excellent fit to enhance ISPC, especially among nurses.

The RQ1 of our study aimed to determine the OCIS factors that can, directly and indirectly, affect employees’ attitude towards ISPC. The RQ1 also sought to determine social bond factors’ mediation role in the relationship between OCIS factors and ISPC. Our findings revealed that OCIS factors significantly affect the social bonding among nurses in an organization. Specifically, the OCIS factor, TMB, has a positive effect on nurses’ commitment, involvement, and personal norms towards organizational infosec issues. The findings are in-line with [28], who advocated that infosec problems emerge mostly because of a lack of interest by top management in organizational IS issues, eventually giving rise to lousy information security culture in an organization [93]. As proved in this study, better TMB can influence employees’ social bonds, and better social bonding between employees creates good infosec culture [12,93,94]. The multi-mediation analysis showed that TMB has a positive effect on the nurses’ attitude. However, the impact was more significant when analyzed through social bond factors such as commitment, involvement, and personal norms. The analysis proved that TMB could increase an individual’s commitment, involvement, and personal norms regarding IS-related issues. These findings are in line with [28]. Therefore, top management from the healthcare organizations can increase employees’ social behaviors towards IS issues, which positively affects employees’ attitude towards ISPC [37].

The results also demonstrated a significant relationship between the other OCIS factor, that is, “organizational control over IS security issues (OCS),” and social bond factors. Among the social bond factors, nurses’ commitment and personal norms were found as significant. These findings are consistent with [28], who argues that the more influential the OCIS factors are, the more likely the organization’s employees bond together to promote organizational ISPC. These findings are consistent with IS and management literature suggesting social bonding enhances organizational performance [18,61,62].

Results also revealed that OCIS factors (i.e., TMB and OCS) have no significant effect on nurses’ attachment which is a different and unexpected finding from previously published research in the same context [11,28]. The best reasons for the failure of these hypotheses have been found from the IS security literature that may be implacable in the current analysis. For instance, ref. [95] explained; employees may perceive rules and regulations imposed by top management as external and consider that ISP is not their prob-
lem [96]. As employees do not have any control over the policies set by top management; therefore, they indulge themselves in a detached behavior called psychological detachment [97]. Moreover, ref. [97] explained that some employees do not like top management involvement in their daily work routine; therefore, they induce detached behavior from the organizational information rules and regulations.

The mediation analysis reveals that OCS showed no significance in enhancing nurses’ involvement in organizational IS security issues. The reason for the failure of this hypothesis has been described in [11]. They have discussed that healthcare administrative control over the IS security issues should be based on the motivations and acceptable training methods. In contrast, if the organizations are not using exact motivation methods to control the IS issues, they may not be involved in IS-related activities as required.

The second research question (RQ2) assessed social bond factors on nurses’ attitude towards ISPC. The findings exhibited that social bond factors can positively affect the nurses’ attitude towards ISPC. There is plenty of literature suggesting that good social bonding between employees improves ISPC [12,18,19]. Our findings implied that commitment has tremendous significance towards the attitude. An employee with a better commitment to organizational security issues likely to have a less deviant attitude towards ISPC [12,19]. In contrast, involvement showed a significant positive relationship with the attitude of nurses. These results are in line with the findings of the study conducted by [19]. Likewise, multiple studies proved that better organizational rules and regulations shape an employee’s positive attitude [12,98].

Personal norm is the last and most useful construct in the framework that influences employees’ intention towards the organizational ISP. The data analysis revealed that personal norms positively affect the intention of nurses to comply with organizational ISPs. This finding is correlated with that of [65] in terms of employees’ ISPC. These findings also mirror the observations reported in similar studies [12,28,98], showing that individuals’ enhanced personal norms towards ISPs promote adherence to IS security rules and regulations.

Further analysis revealed that attachment showed no significant relationship with the attitude of nurses in this context. This result was unexpected because multiple studies have proved otherwise [18,28]. The best reason we have found from the existing literature was explained by [19] by stating that employees may have a positive attitude towards the organizational policies but have different perceptions or views from fellow employees. According to [99], self-interest and perceived benefits are the major causes of such behavior.

This study has examined the mediating effect of social bond factors and attitude toward ISPC in the relationship between TMB and OCS. Our study contributes a noteworthy contribution to the existing body of literature because few studies have examined OCIS factors from the health sector’s organizational climate.

7. Conclusions

This section comprises theoretical contributions, the implication to practice, study limitations, future research, and closing remarks from the authors.

7.1. Theoretical Contributions

This paper offers multiple theoretical contributions to the IS security management literature. To the best of the researcher’s knowledge, this study is among the first studies to incorporate OCIS factors’ effect through the mediation of social bonds for healthcare information security. This integrative research model offers a new perspective for recognizing healthcare employees’ (i.e., nurses’) behavioral intentions. We concluded that this conceptualization complements other widely publicized research focused on punishment-based theories (for example, protection motivation theory, deterrence theory). We believe that this study has provided another insight into why employees do not want to comply because of perceived sanctions or deterrence [10,75].
This study’s multi-mediation model provides a way for integrating the OCIS and social bond theory to assess ISPC. Furthermore, this study supports SBT’s assumptions about the understanding of group pressures and social/personal expectations that can help deter deviant activities from complying with IS security policy compliance. This study offered more empirical evidence for the importance of social bonding, normative values, and workgroup norms to comply with ISPs in work settings. The two constructs from OC (i.e., TMN and OCS) were measured along with the social bond factor to enhance employees’ attitudes towards ISPC. The study endorsed that top management concerns about organizational security problems would improve employee social bonding, thereby fostering ISPC in an organization. Besides, it has been demonstrated that employees often view top management as external involvement and indulge deviant actions towards organizational ISPs [95].

7.2. Practical Contribution

This study presented HIS security practitioners with various practical implications. First, the study indicates that top management control and IS security concerns positively affect employees, such as nurses’ commitment and personal norms, contributing to ISPC in organizations. The findings of RQ1 indicated that the niggling doubts of top management with the ISP enforcement of individuals could result in the psychological detachment of nurses with the IS issues. In this regard, managers should not display any additional concerns about employees’ (i.e., nurses’) everyday work routine; however, reasonable control in this sense may be useful.

Second, OCIS factors are essential for improving social bonding (as indicated by results of RQ2). In this regard, this research suggests that management must take input from all top-level to bottom-level employees when developing ISPs so that all organizational actors can own their ISPs. Results further revealed that OCIS factors could increase employees’ commitment and personal norms, which later foster a thriving infosec culture, especially in healthcare organizations. The top management can consider encouraging a culture where employees’ commitment can be associated with such motivations (i.e., intrinsic and extrinsic). It may be in monthly or quarterly incentives for those who stick to such directions.

Third, social bonding proved to be an essential component to enhance ISPC among healthcare employees such as nurses. Therefore, top management should focus on promoting social bonds among individuals to improve compliance. For instance, top management can seek assistance from prominent individuals who can influence employees’ views and attitudes towards ISPC. Also, employees with a greater understanding of IS practices and attitudes need to be positioned as role models. Those role models’ values can be adopted by other employees [28,58].

The results of this study can help security managers and security practitioners in health organizations. This study’s analysis suggests that managers should concentrate on learning more about information management and ISP-related behavioral problems. Several studies have shown that top management’s views and concerns will strengthen information security culture [18,28]. Moreover, this study’s results revealed that top management beliefs and organizational control over IS security issues could enhance social bonding among employees, especially nurses who later cultivate good information security behaviors in healthcare organizations.

7.3. Limitations and Future Research

Like all empirical studies, this study also has some limitations. First, the full collinearity test has provided enough support, but it is still possible that participants provided socially desirable answers to some of the survey questions. Second, the data was collected from both types of participants who had formal ISPs implemented in their organizations and from others without formal ISPs; it may have detrimental effects on the results to include both groups of respondents. In addition to this, the questionnaire used provided the
respondents with complete information about this study. In the comparison of responses from both groups, no statistically significant difference was observed.

Future research in this field could overcome some of the limitations discussed in this study. First, this is an empirical study; a longitudinal study may improve the results in the future. Second, this framework should be tested with multi-cultural employees to confirm this research’s findings in the future.

Third, the data analysis for this study is based on data collected from nurses at the hospital. Initially, it was aimed at gathering data from doctors. However, detailed safety protocols in each hospital and doctors’ hectic working times during the COVID-19 pandemic have refrained us from collecting doctors’ data. Therefore, our analytical unit is restricted to data from hospital nurses who were available and willing to provide data. Therefore, future studies are encouraged to expand the current research landscape’s effects by including data obtained from health staff, such as doctors, surgeons, information technicians, and other administrative personnel.

7.4. Closing Remarks

Healthcare organizations are considered as one of the most vulnerable organizations in the context of infosec. Healthcare organizations must focus on insider threats and put more effort into implementing behavioral security controls to mitigate insiders’ deviant behaviors. The negligence by employees towards the organization’s ISP is a function of many factors such as unawareness, lack of knowledge, stress, and conflicts. This study has attempted to solve the behavioral infosec problem in healthcare organizations by incorporating OCIS and social bond factors. Although more research is required to increase knowledge about behavioral infosec in the healthcare sector, a persuasive yet effective framework is validated to adapt essential constructs to foster ISPC.

Supplementary Materials: The following are available online at https://www.mdpi.com/2071-1050/13/5/2800/s1.

Author Contributions: Conceptualization K.D., and R.F.A.; methodology, K.D., R.F.A., P.D.D.D.; software, R.F.A.; validation, K.D.; formal analysis, K.D., R.F.A.; data curation, R.F.A. and P.D.D.D.; writing—original draft preparation, R.F.A., S.E.A.A.; writing—review and editing, P.D.D.D. and S.E.A.A.; visualization, R.F.A.; supervision, P.D.D.D.; project administration, R.F.A. and P.D.D.D.; funding acquisition, K.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by YUTP-FRG Grant (015LCO-171).

Institutional Review Board Statement: Ethical review and approval were waived for this study as this was a survey analysis with questions about work practices. Importantly, we did not ask employees any questions that could jeopardize their privacy or confidentiality. As a result, all of the respondents voluntarily participated in this report.

Informed Consent Statement: Informed consent was obtained from all participants involved in the study.

Data Availability Statement: Data is contained within the supplementary material.

Acknowledgments: The authors would also like to thank the anonymous reviewers for their valuable suggestions to enhance the manuscript. We would also like to thank the Department of Computer and information Sciences, Universiti Teknologi PETRONAS, Malaysia, for facilitating this research study.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Mantzana, V.; Darra, E.; Gkotsis, I. Cyber-Physical Security in Healthcare. In Safety and Security Issues in Technical Infrastructures; IGI Global: Hershey, PA, USA, 2020; pp. 63–87.
2. Ali, S.E.A.; Lai, F.-W.; Hassan, R.; Shad, M.K. The Long-Run Impact of Information Security Breach Announcements on Investors’ Confidence: The Context of Efficient Market Hypothesis. Sustainability 2021, 13, 1066. [CrossRef]
3. Syed, E.; Azhar, A.; Fong-Woon, L.; Rohail, H. Socio-Economic Factors on Sector-Wide Systematic Risk of Information Security Breaches: Conceptual Framework. In Proceedings of the International Economics and Business Management Conference, Melaka, Malaysia, 2–3 November 2020; pp. 502–512.

4. Brady, J.W. Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers. In Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 4–7 January 2011; IEEE: New York, NY, USA, 2011; pp. 1–10.

5. Naseer, S.; Ali, R.F.; Dominic, P.; Saleem, Y. Learning Representations of Network Traffic Using Deep Neural Networks for Network Anomaly Detection: A Perspective towards Oil and Gas IT Infrastructures. *Symmetry* 2020, 12, 1882. [CrossRef]

6. Chen, L.; Zhen, J.; Dong, K.; Xie, Z. Effects of sanction on the mentality of information security policy compliance. *Rev. Argent. Clínica Psicológica* 2020, 29, 39–49.

7. Bansal, G.; Muñatxo, S.; Shin, S.I. Information system security policy noncompliance: The role of situation-specific ethical orientation. *Inf. Technol. People* 2020, 34, 250–296. [CrossRef]

8. Corradini, I. *Building a Cybersecurity Culture in Organizations*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 23–47.

9. Năstase, P.; Năstase, F.; Ionescu, C. Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Econ. Comput. Econ. Cybern. Stud. Res.* 2009, 43, 1–16.

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

11. Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics J.* 2019, 26, 461–473. [CrossRef]

12. Ali, R.F.; Dominic, P.; Ali, K. Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective towards Oil and Gas Employees. *Sustainability* 2020, 12, 8576. [CrossRef]

13. Chakraborty, T.; Jajodia, S.; Katz, J.; Picariello, A.; Sperli, G.; Subrahmanian, V.S. FORGE: A Fake Online Repository Generation Engine for Cyber Deception. *IEEE Trans. Dependable Secur. Comput.* 2019, 1. [CrossRef]

14. Amato, F.; Moscato, V.; Picariello, A.; Sperli, G. Multimedia Social Network Modeling: A Proposal. In Proceedings of the 2016 IEEE Tenth International Conference on Semantic Computing (ICSC), Laguna Hills, CA, USA, 4–6 February 2016; IEEE: New York, NY, USA, 2016; pp. 448–453.

15. Hina, S.; Selvam, D.D.D.P.; Lowry, P.B. Institutional governance and protection motivation: Theoretical insights into shaping employees’ security compliance behavior in higher education institutions in the developing world. *Comput. Secur.* 2019, 87, 101594. [CrossRef]

16. IBM. Security Services. IBM Infographic: Cyber Security Intelligence Index. 2014. Available online: http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic (accessed on 4 May 2014).

17. Gwebu, K.L.; Wang, J.; Hu, M.Y. Information security policy noncompliance: An integrative social influence model. *Inf. Syst. J.* 2019, 30, 220–269. [CrossRef]

18. Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence and cognition. *Inf. Manag.* 2014, 51, 69–79. [CrossRef]

19. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* 2016, 56, 70–82. [CrossRef]

20. Cheng, L.; Li, Y.; Li, W.; Holm, E.; Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Comput. Secur.* 2013, 39, 447–459. [CrossRef]

21. Appari, A.; Johnson, M.E. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Entrep. Manag.* 2010, 6, 279. [CrossRef]

22. Mishra, S.; Caputo, D.J.; Leone, G.J.; Kohun, F.G.; Draus, P.J. The Role of Awareness and Communications in Information Security Management: A Health Care Information Systems Perspective. *Int. J. Manag. Inf. Syst. (IJMIS)* 2014, 18, 139. [CrossRef]

23. Hedström, K.; Karlsson, F.; Kolkowska, E. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Inf. Manag. Comput. Secur.* 2013, 21, 266–287. [CrossRef]

24. Van Deursen, N.; Buchanan, W.J.; Duff, A. Monitoring information security risks within health care. *Comput. Secur.* 2013, 37, 31–45. [CrossRef]

25. Samy, G.N.; Ahmad, R.; Ismail, Z. Security threats categories in healthcare information systems. *Health Informatics J.* 2010, 16, 201–209. [CrossRef] [PubMed]

26. Renaud, K.; Goucher, W. Health service employees and information security policy securities: An uneasy partnership? *Inf. Manag. Comput. Secur.* 2012, 20, 296–311. [CrossRef]

27. Alanazi, S.T.; Anbar, M.; Ebad, S.A.; Karuppayah, S.; Al-Ani, H.A. Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry* 2020, 12, 1544. [CrossRef]

28. Ifinedo, P. Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. *Inf. Resour. Manag. J.* 2018, 31, 53–82. [CrossRef]

29. Azhar Ali, S.E.; Khurram, S. Impact of Demographic and Health Factors on GDP Growth of South Asian Countries. *Int. J. Acad. Res. Bus. Soc. Sci.* 2017, 7, 2222–6990.
30. Shahri, A.B.; Ismail, Z.; Rahim, N.Z.A. Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems. J. Teknol. 2013, 64, 7–12. [CrossRef]
31. Humaidi, N.; Balakrishnan, V. Exploratory factor analysis of user’s compliance behaviour towards health information system’s security. J. Health Med. Inform. 2013, 4, 2–9. [CrossRef]
32. Humaidi, N.; Balakrishnan, V. The Moderating effect of working experience on health information system security policies compliance behaviour. Malays. J. Comput. Sci. 2015, 28, 70–92.
33. Mark, G.; Schneider, E.B.; William, H.M. Organizational Climate and Culture: An Introduction to Theory, Research, and Practice; Routledge: Boca Raton, FL, USA, 2013.
34. Joyce, W.E.; Slocum, J.W. Climates in organizations. Organ. Behav. 1979, 2, 1–11.
35. Neal, A.; Griffin, M.; Hart, P. The impact of organizational climate on safety climate and individual behavior. Saf. Sci. 2000, 34, 99–109. [CrossRef]
36. Brown, S.P.; Leigh, T.W. A new look at psychological climate and its relationship to job involvement, effort, and performance. J. Appl. Psychol. 1996, 81, 358–368. [CrossRef] [PubMed]
37. Humaidi, N.; Balakrishnan, V. Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. Int. J. Inf. Technol. 2015, 5, 311–318. [CrossRef]
38. Jaafar, N.I.; Ajis, A. Organizational climate and individual factors effects on information security compliance behaviour. Int. J. Bus. Soc. Sci. 2013, 4, 118–130.
39. Safa, N.S.; Maple, C.; Furnell, S.; Azad, M.A.; Perera, C.; Dabbagh, M.; Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Comput. Syst. 2019, 97, 587–597. [CrossRef]
40. Ghazvini, A.; Shukur, Z. A Framework for an Effective Information Security Awareness Program in Healthcare. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 193–205. [CrossRef]
41. Humaidi, N.; Balakrishnan, V. Indirect effect of management support on users’ compliance behaviour towards information security policies. Health Inf. Manag. J. 2017, 47, 17–27. [CrossRef]
42. Albarakk, A.I. Information security behavior among nurses in an academic hospital. J. Soc. Dev. New Net Environ. B&H 2012, 6, 2349–2354.
43. Michel-Verkerke, M.B. Information Quality of a Nursing Information System depends on the nurses: A combined quantitative and qualitative evaluation. Int. J. Med. Informatics 2012, 81, 662–673. [CrossRef] [PubMed]
44. Ferdousi, R.; Arab-Zozani, M.; Tahamtan, I.; Rezaei-Hachesu, P.; Dehghani, M. Attitudes of nurses towards clinical information systems: A systematic review and meta-analysis. Int. Nurs. Rev. 2020, I. [CrossRef]
45. Baghini, M.S.; Baniasadi, N. Evaluation of Nursing Information System: Nurses’ Perspectives. Appl. Health Inf. Technol. 2021, 1. [CrossRef]
46. Kuo, K.-M.; Talley, P.C.; Hung, M.C.; Chen, Y.-L. A Deterrence Approach to Regulate Nurses’ Compliance with Electronic Medical Records Privacy Policy. J. Med. Syst. 2017, 41, 1–10. [CrossRef]
47. Martikainen, S.; Kaipio, J.; Lääveri, T. End-user participation in health information systems (HIS) development: Physicians’ and nurses’ experiences. Int. J. Med. Informatics 2013, 137, 104117. [CrossRef]
48. Kroll Advisory Solutions. HIMSS Analytics Report: Security of Patient Data. 2012. Available online: https://www.kroll.com/en/insights/publications/himss-patient-data-security-study (accessed on 4 April 2012).
49. Dimitropoulos, L.; Rizk, S. A State-Based Approach to Privacy and Security for Interoperable Health Information Exchange. Health Aff. 2009, 28, 428–434. [CrossRef]
50. Colwill, C. Human factors in information security: The insider threat—Who can you trust these days? Inf. Secur. Tech. Rep. 2009, 14, 186–196. [CrossRef]
51. Donahue, K.; Rahman, S. Healthcare IT: Is your Information at Risk? Int. J. Netw. Secur. Its Appl. 2015, 4, 97–109. [CrossRef]
52. Shahri, A.B.; Ismail, Z.; Mohanna, S. The Impact of the Security Competency on “Self-Efficacy in Information Security” for Effective Health Information Security in Iran. J. Med. Syst. 2016, 40, 1–9. [CrossRef] [PubMed]
53. Cram, W.A.; D’Arcy, J.; Proudfoot, J.G. Seeing the forest and the trees: A meta-analysis of the antecedents to information security policies compliance. MIS Q. 2019, 43, 525–554. [CrossRef]
54. Malimage, K.; Raddatz, N.; Trinkle, B.S.; Crossler, R.E.; Baaske, R. Impact of Deterrence and Inertia on Information Security Policy Changes. J. Inf. Syst. 2020, 34, 123–134. [CrossRef]
55. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. MIS Q. 2018, 42, 285–312. [CrossRef]
56. Ali, R.F.; Dominic, D.D.D.; Karunakaran, P.K. Information security policy and compliance in oil and gas organizations—A pilot study. Solid State Technol. 2020, 63, 1275–1282.
57. Syed, E.A.A.; Syed, S.H.R.; Fong-Woon, L.; Rao, F.A.; Ahmad, A.J. Predicting Delinquency on Mortgage Loans: An Exhaustive Parametric Comparison of Machine Learning Techniques. Int. J. Ind. Eng. Manag. 2021, 12, 1–13.
58. Ifinedo, P. Socio-Economic correlates of information security threats and controls in global financial services industry: An analysis. Int. J. Inf. Serv. Serv. Sect. 2015, 7, 54–70. [CrossRef]
59. Rota, C.; Reynolds, N.; Zanasi, C. The influence of organizational climate on sustainable relationships between organization and employees. The KION case study. Adv. Manag. Appl. Econ. 2012, 2, 126–140.
60. Joyce, W.F.; Slocum, J.W. Jr. Collective climate: Agreement as a basis for defining aggregate climates in organizations. *Acad. Manag. J.* 1984, 27, 721–742.

61. Shadur, M.A.; Kienzle, R.; Rodwell, J.J. The relationship between organizational climate and employee perceptions of involvement: The importance of support. *Group Organ. Manag.* 1999, 24, 479–503. [CrossRef]

62. McMurray, A.J.; Scott, D.R.; Pace, R.W. The relationship between organizational commitment and organizational climate in manufacturing. *Hum. Resour. Dev. Q.* 2004, 15, 473–488. [CrossRef]

63. Shahzad, K.; Shareef, K.; Ali, R.F.; Nawab, R.M.A.; Abid, A. Generating process model collection with diverse label and structural features. In *Proceedings of the 2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Dublin, Ireland, 24–26 August 2016; IEEE: New York, NY, USA, 2016; pp. 644–649.

64. Asch, S.E. Opinions and Social Pressure. *Sci. Am.* 1951, 185, 31–35. [CrossRef]

65. Yazdanmehr, A.; Wang, J. Employees’ information security policy compliance: A norm activation perspective. *Decis. Support Syst.* 2016, 92, 36–46. [CrossRef]

66. Berg, M. Patient care information systems and health care work: A sociotechnical approach. *Int. J. Med Informatics* 1999, 55, 87–101. [CrossRef]

67. Hirschi, T.; Stark, R. Hellfire and Delinquency. *Soc. Prob. 1969*, 17, 202–213. [CrossRef]

68. Watt, B.; Howells, K.; Delfabbro, P. Juvenile recidivism: Criminal propensity, social control and social learning theories. *Psychiatry Psychol. Law* 2004, 11, 141–153. [CrossRef]

69. Ali, K.; Johl, S.K. Impact of nurse supervisor on social exclusion and counterproductive behaviour of employees. *Cogent Bus. Manag.* 2020, 7, 1–19. [CrossRef]

70. Steers, R.M. Antecedents and Outcomes of Organizational Commitment. *Adm. Sci. Q.* 1977, 22, 46. [CrossRef]

71. Robinson, S.L.; O’Leary-Kelly, A.M. Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Acad. Manag. J.* 1998, 41, 688–672.

72. Chan, M.; Woon, I.; Kankanhati, A. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *J. Inf. Priv. Secur.* 2005, 1, 18–41. [CrossRef]

73. Dewe, P.J.; O’Driscoll, M.P.; Cooper, C. *Coping with Work Stress: A Review and Critique*; John Wiley & Sons: Hoboken, NJ, USA, 2010.

74. Lee, S.M.; Yoo, S. An integrative model of computer abuse based on social control and general deterrence theories. *Inf. Manag.* 2004, 41, 707–718. [CrossRef]

75. Herath, T.; Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* 2009, 18, 106–125. [CrossRef]

76. Taylor Davis & Connor Bice, The Nurse EHR Experience: An Arch Collaborative Impact Report, Arch Collaborative. 28 March 2019. Available online: https://klasresearch.com/archcollaborative/report/the-nurse-ehr-experience/260 (accessed on 28 March 2019).

77. Ministry of Health. Malaysia Report, Human Resource for Health (HRH) Malaysia. 2020. Available online: http://www.moh.gov.my/index.php/pages/view/1919?mid=626 (accessed on 19 March 2020).

78. Krejcie, R.V.; Daryle, W. Determining sample size for research activities. *Educ. Psychol. Meas.* 1970, 30, 607–610. [CrossRef]

79. Hair, J.F.; Ringle, C.M.; Sarstedt, M. Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. *Long Range Plan.* 2013, 46, 1–12. [CrossRef]

80. Ifinedo, P. Understanding information systems policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* 2012, 31, 83–95. [CrossRef]

81. Hair, J.F.; Hollingsworth, C.L.; Randolph, A.B.; Chong, A.Y.L. An updated and expanded assessment of PLS-SEM in information systems research. *Ind. Manag. Data Syst.* 2017, 117, 442–458. [CrossRef]

82. Sijtsma, K. Reliability Beyond Theory and Into Practice. *Psychometrika* 2008, 74, 169–173. [CrossRef]

83. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* 2015, 43, 115–135. [CrossRef]

84. Hair, J.F.; Sarstedt, M.; Ringle, C.M. Rethinking some of the rethinking of partial least squares. *Eur. J. Mark.* 2019, 53, 566–584. [CrossRef]

85. Hu, L.T.; Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struct. Equ. Model.* 1999, 6, 1–55. [CrossRef]

86. Bryman, A. *Social Research Methods*, 2nd ed.; Oxford University Press: Oxford, UK, 2016.

87. Hair, J.F., Jr.; Tomas, G.; Hult, M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed.; Sage Publications: Thousand Oaks, CA, USA, 2016.

88. Nitzl, C.; Roldán, J.L.; Cepeda, G. Mediation analysis in partial least squares path modeling: Helping researchers discuss more sophisticated models. *Ind. Manag. Data Syst.* 2016, 116, 1849–1864. [CrossRef]

89. Carrion, G.C.; Nitzl, C.; Roldán, J.L. *Mediation Analyses in Partial Least Squares Structural Equation Modeling: Guidelines and Empirical Examples*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2017; pp. 173–195.

90. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed.; Academic Press: Cambridge, MA, USA, 1988.

91. Kock, N. *Common method bias in PLS-SEM: A full collinearity assessment approach*. *Int. J. e-Collaboration* 2015, 11, 1–10. [CrossRef]

92. Merhi, M.I.; Ahluwalia, P. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Comput. Hum. Behav.* 2019, 92, 37–46. [CrossRef]
93. Nasir, A.; Arshah, R.A.; Ab Hamid, M.R.; Fahmy, S. An analysis on the dimensions of information security culture concept: A review. *J. Inf. Secur. Appl.* 2019, 44, 12–22. [CrossRef]

94. Bye, A. Defining and Developing a Model for an Engaged Information Security Culture; Technical Report; Royal Holloway University of London: London, UK, 2018.

95. D’Arcy, J.; Herath, T.; Shoss, M.K. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *J. Manag. Inf. Syst.* 2014, 31, 285–318. [CrossRef]

96. D’Arcy, J.; Teh, P.-L. Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Inf. Manag.* 2019, 56, 103151. [CrossRef]

97. Xu, Z.; Guo, K. It ain’t my business: A coping perspective on employee effortful security behavior. *J. Enterp. Inf. Manag.* 2019, 32, 824–842. [CrossRef]

98. Ifinedo, P. Investigating employee engagement in nonmalicious, end-user computing and information security deviant behavior. In Proceedings of the Twenty-Fifth Americas Conference on Information Systems, Cancún, Mexico, 4 July 2019; pp. 1–10.

99. Casper, W.J.; Harris, C.M. Work-life benefits and organizational attachment: Self-interest utility and signaling theory models. *J. Vocat. Behav.* 2008, 72, 95–109. [CrossRef]