THE MODERATING EFFECT OF WORKING EXPERIENCE ON HEALTH INFORMATION SYSTEM SECURITY POLICIES COMPLIANCE BEHAVIOUR

Norshima Humaidi[1], Vimala Balakrishnan[2]

[1]Faculty of Business Management, University of Technology MARA 42300, PuncakAlam Campus, Selangor, Malaysia.
[2]Faculty of Computer Science and Information Technology, University of Malaya, 50603, Kuala Lumpur, Malaysia.

Email: [1]norshima24@yahoo.com,[2]vimala.balakrishnan@um.edu.my

ABSTRACT

This study was conducted to investigate the moderating effect of health professional's working experience on the relationship between factors of Health Information System Security Policies Compliance Behaviour (HISSPC) model. A survey (i.e., n = 454) was conducted to test the differences between high experience and low experiencehealth professionals who were Health Information System (HIS) users. The HISSPC model was tested using partial least squares (PLS) approachwith results indicating the coefficient of determination (i.e., R^2) for high experience group (i.e., 63 percent)to be slightly higher than the low experience group(i.e., 60 percent). Statistical differences were noted for the relationship between management support and user's compliance behaviour in both groups,with stronger relationship forlow experienceHIS users compared to high experience HIS users. In contrast, perceived susceptibility was found to significantly influence highly experienced users to comply with HIS security policies, however it had no significant effect for the low experience group.The overall moderating effect size for high experience userswas approximately 0.07 (i.e. small) andno moderating effect was observed for the low experience group (i.e., f^2 = 0.01). It was believed that the findings will provide better guidelines to fellow researchers and policy makers in improving information security behaviour among health professionals in hospitals, particularly those with varying working experiences.

Keywords: Health information system; working experience; information security policies; compliance behavior; information security; multi-group analysis

1.0 INTRODUCTION

Health Information System (HIS) improvesthe filing system in health institutions. Although HIS is an example of innovative product towards effective healthcare delivery, it has a higher degree of vulnerability towards the threats of information security such as unauthorized access, use, disclosure, disruption, modification or destruction and duplication of passwords. This could be due to the greater openness of multi-connectedness between heterogeneous stakeholders within the networks. Information security threat is defined as undesirable incidents that can cause different types of damage, which might lead to the loss of an organization's finances or reputation [1]. Therefore, information security plays an important role to protect health data from information security threat [2]. The main information security threat in the organization is internal threat, which is caused by employees of the organization[3-4]. The employees have legitimate and often privileged access to facilities and organization information, have knowledge of the organization and its processes and know the location of critical or valuable assets [5]. One of the major internal threatin the organization is human error.Many human errors reported in the previous studies are caused by accidental acts because of user slips and mistakes due to a lack of information concerning security skills and lack of knowledge towards information security [6-8]. Human slips occur as an outcome of the incorrect execution of a correct action sequence, which usually happens because of human carelessness, such as inadequate written communication (e.g., prescriptions, documentation, transcription) [9]. Meanwhile, human mistakes occur as an outcome of the correct execution of an incorrect action sequence, i.e., wrong decisions executed correctly because of human ignorance, and failure to comply with an organization's rules and procedures [10]. For an example, the behaviour like sharing password with other people. This is supported by other studies, in which human error occurs when a person fails to take the correct action that is required, especially when implementing information security policies(ISPs)[11]. For example, one who forgets to back up a hard disk or does not create a

strong password. Therefore, top management should consider and invest not only in the technical part of the system, but also in the human resources.

ISPs highlight the importance of information security aspects such as how to protect valuable information [12] and help to reduce the number of security incidents in an organization [13]. However, security incidents cannot be reduced if employees are not aware of the existence of ISPs[14]. Thus, information security awareness among employees is very important in organizations because of its capability to reduce occurrences of security incidents [15-16]. Previous literatures have argued that management is responsible in developing security awareness among their employees in the organization [17]. This can be done through conducting information security training and on-going security campaign program. Through effective training and education, employees' behaviour and information security skills can be improved as employees are encouraged to have good information security practices as recommended by their organisations [18]. Meanwhile, authors of other literatures argued that security awareness campaign affects employees' compliance behaviour towards information security [15, 19]. The campaign can help employees to be alert to any current information related to information security threat, and also to new security policies that have been/will be implemented.

In other empirical studies, it has been argued that employees who have experience with information security incident, and aware of the consequences of non-compliance behavior such as loss of job and severe penalty, will be more careful and adopt acceptable security behavior as recommended by organizations [20-22]. Research findings by Li et al. [23] indicated that employees' intention, when complying with security policies, involves a cost-benefit analysis. According to the authors, employees are more likely to comply with security policies when perceived benefits are overridden by potential risks of formal sanctions and security threats. Other studies highlighted that employees must recognize information security threat and the risk these threats pose to their organizations [21]; based on this awareness, they might comply with ISPs and practice security behaviour appropriately. However, employees' compliance behavior towards ISPs might reduce if they feel adhering to the security policies is time consuming [17]. This situation usually happens when employees have to work under pressure, such as when trying to meet deadlines [20].

Apart from information security awareness, trust and security barrier are also factors of user adherence to organization's ISPs. It has been suggested that trust should be explored in studies related with information security compliance behavior in healthcare industry[24]. This is also argued by previous literature that an individual's compliance behavior towards rules and regulations can be improved if fostered by the trustworthiness of policymakers [25]. Therefore, management who are also the policymaker needs to foster confidence towards ISPs to all employees in the organization to ensure that information security objectives are achieved. Meanwhile, barrier in information security is related to unskilled employees towards security technology due to a lack of security knowledge. Knowledge is usually developed through user's working experience on the particular environment [26]. Moreover, the degree of difficulty users experience in complying with the policies and procedures can influence their compliance behaviour [27]. If performing information security requires time and effort, then employees will be less likely to perform information security requirements [28]. This probably takes place as employees have to work under extreme pressure to finish their work [17], especially in healthcare environment, in which health professionals have to serve many patients almost every day.

This study fills the research gap between different constructs of management support and ISPs compliance behaviour. Although the role of management has been used extensively to evaluate the links between employees' behaviour and technological effectiveness in the Malaysian culture, none of them has connected managerial supportwith HIS security policies through compliance behaviour. This study has emphasized the consideration on dual aspects of managerial support (i.e., leadership behaviour and information system security training) in evaluating the patterns of compliance behaviour among health professionals with different levels of working experience. Employeeswith greater working experiences is said to be more knowledgeable than those with low working experiences[29]. However, does working experiencemoderate the impact of management support on user's compliance behaviour? Bearing this issue in mind, this paper aims to investigate the moderating effect of working experience of health professionalson the relationship between management support and user's ISP compliance behaviour. Additionally, this study also investigates other human factors related to compliance behaviour. The objectiveisaccomplished by developing Health Information System Security Policy Compliance Behaviour (HISSPC) model, which is an integration of Theory of Planned Behaviour (TPB) and Health Belief Model (HBM).

The paper begins with a discussion of theoretical conception for developing an integrated research model that can be tested empirically. Next, we discuss the development of HISSPC model and hypotheses. Thereafter, we discuss the

research methodology adopted in the current study. Finally, the findings of the study are presented and discussed, and the paper is concluded with the implications of the study and recommendations for future research.

2.0 THEORETICAL BACKGROUND

The current study attempts to understand the moderating effect of health professional's working experiences on the relationship between the indicated factors (i.e.,management support, information security awareness, security barrier, information system (IS) skills and trust) and ISPs compliance behaviour. We have investigated several theoretical backgrounds that have been adapted from previous ISPs compliance behaviourstudies such as Protection Motivation Theory (PMT) [22, 30], Theory of Planned Behaviour (TPB) [20, 27-28] and Deterrence Theory [22, 31], among others. In the current study, TPB and HBM are combined to develop a HISSPC model because both theories are widely known in human behaviour studies in the domains of both healthcare and information security.

Table 1: Characteristics of theories

Theories/Characteristics	**Health belief Model (HBM)**	**Theory of Planned Behavior (TPB)**
Years	1950s	1985s by IcekAjzen
Description of the theory	HBM isdeveloped to explain and predict preventative health behaviours [33]	TPB has been applied extensively to examine users' acceptance of information system which is designed to predict human behavior.
Applications	Health behaviour studies such as those concerning drugs [34], cancers [35], and dental health [36]. Computer security study [32].	Users' acceptance of information system [37-38]. Regulation compliance behaviour among people [30, 39].
Constructs	*Definition of the constructs* Perceived susceptibility: Person's evaluation of his or her probability of being exposed to malicious threats [32] Perceived severity.: An individual's belief in the seriousness of certain circumstances [35] Perceived benefit: To what the person perceives as the positive outcomes of performing certain health behaviors[35] Perceived barrier.: Person's evaluation "of the potential obstacles that may lessen the likelihood of engaging in healthy behavior" [40]	*Definition of the constructs* Subjective norms: Users' perceptions of other people's opinions in terms of whether or not he/she should adopt appropriate behaviour [41] Perceived behavioural control (PCB): Users' perceptions of his/her ability [42], which can be increased through education and training provided by management. Attitude: The degree to which the person has a favorable or unfavorable evaluation of the behavior in question [43]
Previous findings	Perceived susceptibility has also been shown as a determinant of computer security behaviour [32] and also to evaluate a person's probability of being exposed to the malicious threat [44]. Perceived severity isalso reported to influence employees' behaviour towards complying with ISPs [30]. Previous studies have found that the perceived benefit determines information security behaviour [32]. If users feel that adopting information security behaviour is difficult and slowing down their daily works, then it will cause non-compliance behaviour of ISPs among employees in the organization [32]	Previous empirical findings have indicated that superior behaviour has most impact on employees' information security behaviour [30, 41]. Leader in the organization should show positive security behaviour and encourages employees' to comply with ISPs [20], thus, adequate security culture in the organizations can be inculcated. PCB construct has significant affect on users' intention to comply with ISPs [28]. Similar finding isnoted in other studies [16]. PCB components such as education and training programmes can develop user's information security awareness [45] and enhance user's skills to use security tools [46], which lead to improvement of user's compliance behaviour with ISPs.

HBM is a comprehensive healthcare theory because it consists of a number of constructs that are not represented in IS adoption or other theories, but are important in IS security [32]. Previous studies show that HBM is a relevant theory to be adopted in IS security studies because the characteristics of preventive health care (e.g., observing a healthy diet to avoid bad diseases) and protective behaviour (e.g., using a strong password to prevent unauthorised access) are similar [30, 32]. The difference between the studies is that one is used to reduce the effect of diseases while the other is used to reduce the risk of security incidents.

Meanwhile, TPB is the most significant model, which is used to explain user behaviours in IS studies [30]. Since the current study focuses on management support (e.g., superior behaviour, security training, programmes, and implementation of ISPs), information security awareness (e.g., awareness of threat susceptibility, threat severity and benefit of security-countermeasure), self-efficacy, security barrier and trust in the organization's ISPs, the combination of TPB, HBM and trust factor is deemed to be most appropriate in this study. The trust factor in relation to information security behaviour has not been explored much. Trust in the organization's ISPs can improve compliancy with ISPs among employees [28]. Hence, we believe HISSPC provides a detailed theory of human behaviour, which is valuable for understanding compliance behaviour with respect to information security policies in the Malaysian healthcare environment. The characteristics of these theories are explained in Table 1.

3.0 RESEARCH MODEL AND HYPOTHESES

The HISSPC model (i.e., Fig. 1) developed for this study consists of three exogenous constructs (i.e., management support, perceived barrier, and perceived trust). The following indicators are used to measure management support: leadership's behaviour, information security training and ISPs implementation. Information security awareness and self-efficacyare adapted as mediators. Information security awareness consists of three intervening constructs (i.e., perceived severity, perceived susceptibility, andperceived benefit). Meanwhile, the endogenous construct in the current study is HIS users' compliance behaviortowards ISPs, whilst working experience in healthcare environmentisused as the moderator.

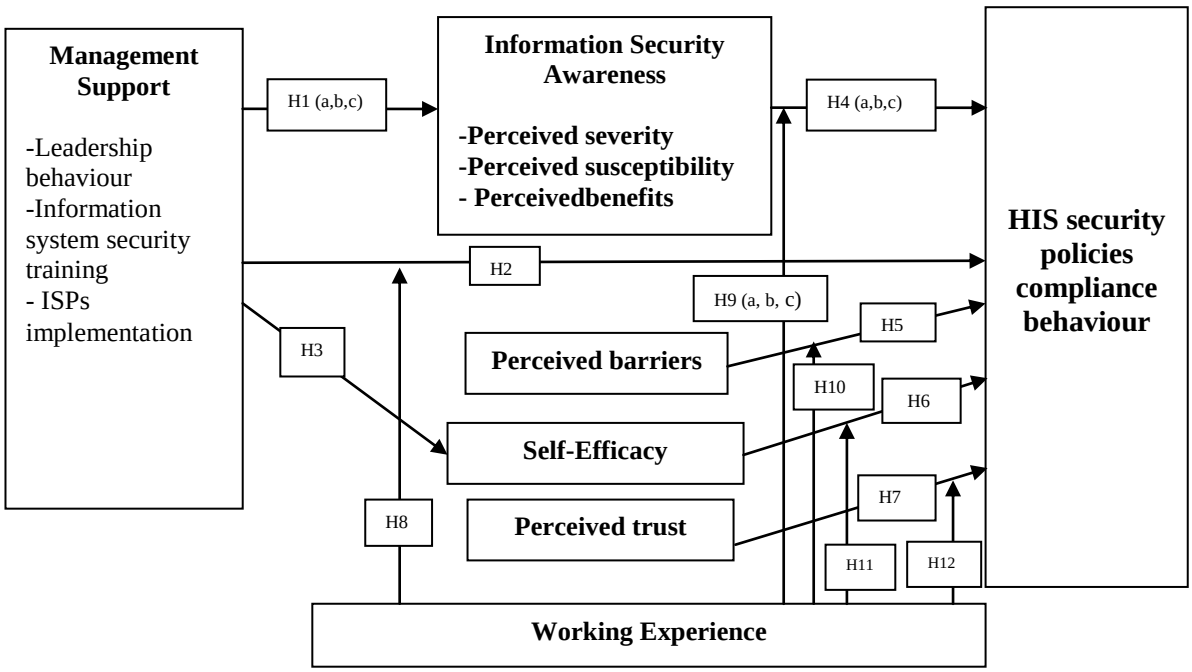


Fig. 1: HISSPC Model

3.1 Management support

Management Support is described as users' perception of the commitment of top management to protect information; one of the critical security components [47]. It is essential that top management play their supportive roles well to ensure effectiveness of information system's security through their leadership behaviour. Management support is also necessary for implementation of ISPs, provision of sufficient information security training and running of effective security awareness programmes for workers. In this study, management support is measured based on TPB constructs (i.e., social pressures and organizational resources).

The social pressures in TPB are called subjective norms, which can be defined as the views of those people who are important to an employee that will affect the employees's behaviour [20]. One of the constructs under social pressure is superior behaviour. The behaviour of superiors is a style of leadership focusing on how leaders monitor and control employees to ensure that they are aware of organization's ISPs. Leadership is defined as the process of influencing others to follow rules and procedures to achieve objectives, whereas leadership style refers to the characteristics of leaders to monitor and control their followers [48-49]. Many leadership studies have shown that both leadership and leadership styles have significant influence on employees' work performance [50]. Strong leadership is required in guiding users to make the right decisions and to promote information security awareness among users. Therefore, the following hypotheses are constructed:

H1a: Management support influences user's awareness of perceived severity.
H1b: Management support influences user's awareness of perceived susceptibility.
H1c: Management support influences user's awareness of perceived benefit of security-countermeasure.

Information security training and ISPs implementation is one of the methods to inform employees about organisations' ISPs [46, 51] which aims to introduce and provide information about the importance of complying with ISPs. Well-managed security training programmes can educate employees to comply with ISPs; therefore, management must ensure that sessions of security training in their organisations are conducted efficiently and any changes on ISPs are alerted to all employees. Moreover, the training can develop employee's information security skills.Based on the above reviews, it can be noted that management support affects users' information security compliance behaviour and user's self-efficacy. Therefore, the following hypotheses are highlighted:

H2: Management support influences user's ISPs compliance behavior.
H3: Management support influences user's self-efficacy.

3.2 Information security awareness (i.e., perceived severity, perceived susceptibilityand perceived benefit)

Perceived severity is the users' perceptions on the seriousness of potential damages or threats [32]. Many empirical studies report that perceived severity of security incidents causes people to behave in a more cautious manner if their degree of perceptions of potential damage or danger increases [30, 52]. Therefore, we formulate the following hypothesis.

H4a: User's awareness of perceived severity influences user's ISPs compliance behaviour.

Meanwhile, perceived susceptibility classified as the subjective risks assessment on information threats [44]. The perceptions of risks and the actions deal with the variations of judgements among the individuals [32]. The number of information security incidents can be reduced if employees are aware of the risk of information security threats to health data. If high susceptibility is perceived by employees, they will be motivated to adopt information security behaviours [53]. Thus, the following hypothesis isconstructed.

H4b: User's awareness of perceived susceptibility influences user's ISPs compliance behaviour.

On the other hand, perceived benefits refers to users subjective beliefs on the benefits [32] of the courses of actions to reduce security threats using appropriate security counter-measures adequately [35]. We believe that when people are aware that the benefits of implementing information protection mechanism and information assets outweigh the cost of protecting them, they are more likely to enact security practices, and vice versa [52]. Therefore, the following hypothesis isdeveloped.

H4c: User's awareness of perceived benefit of security-countermeasure influences user's ISPs compliance behaviour.

We believe that if management monitors HIS users efficiently and provides effective information security programmes and training, users will be more aware of the benefits of security-countermeasure as well as susceptibility and severity of information threats. Thus, they are able to comply with and practice information security policies properly, leading to reduction in the number of security incidents.

3.3 Perceived barrier

Ng et al. [32] defines perceived barrier as a user's perceptions towards the difficulty of practicing information security behaviour, which is likely to reduce the performance of information security behaviour among users. The barriers in information security is the reason why employees did not practice computer security in their workplaces [32]. This study refers to security barriers as any costs related to taking adaptive action, such as monetary, time, effort, inconvenience and complexity [54]. If employees feel that complying with organization's ISPs are slowing down their work, then they will be less likely to perform compliance behaviour [22]. This leads to the following hypothesis:

H5: Perceived barrier influences user's ISPs compliance behaviour.

3.4 Self-Efficacy

Self-efficacy actually originates from Social Cognitive Theory [55] which determines how people feel, think, and motivate them to behave in a certain way based on cognitive, motivational, affective, social influence, and selection processes [52]. According to Chan et al. [56], people self-efficacy can develope through the ongoing acquisition of knowledge. Furthermore, this knowledge can be gained through experience with the certain subject or event. Self-efficacy of users can be enhanced through training programmes provided by the management in the organization [57].

Self-efficacy in the current study is related with employee's information security skills which is defined as user's perception about their computer security skills that can motivate them to behave in a certain way. Self-efficacy can be enhanced through information security awareness programmes and training, which aim to introduce and provide information about the importance of information system's security and to increase users' skill toward using security-countermeasure [58]. Thus, the following hypothesis is constructed:

H6: Self-efficacy influences user's ISPs compliance behaviour.

3.5 Perceived trust

Trust which is defined as how users feel about security and their willingness to adopt IThad been widely used in e-commerce researches, [59]. Perceived trust also has been used in information technology studies to investigate issues of information security and privacy [60]. Perceived trust in the current study refers to users expected confidence on the implementation of security policies through managerial support.Previous empirical findings reported that trust positively affects consumer behavior intention to use online transaction [59, 61] and a powerful predictor on information security behaviour among employees [3]. Trust is an important factor in social relationship, and a lack of trust among people will lead to lesser performance on a social as well as academic and professional level [62].

The trust of health professionals' in the management of health institutions will enhance their compliance behaviour with ISPs related to HIS use. Therefore, perceived trust is considered as one of the constructs that can affect users' compliance behaviour towards HIS policies, therefore the following hypothesis is developed.

H7: Perceived trust influences user's ISPs compliance behaviour.

3.6HIS experience as a moderator in user's compliance behavior towards ISPs

Experience is related to individual abilities, knowledge and skills, which are developed through formal or informal education [26]. Shen et al. [63] referred to experience as the knowledge or skills that people obtain through the involvement in or exposure to a particular event. The moderating effect of usage experience in IS has been widely investigated in e-commerce studies, such as users' technology acceptance [64] and users' behavioural intention [63, 65]. Both of the previous studies have shown that users' experiences with IS moderate the effect of users' intention to use the technology.

The currentstudy considers users' working experience at handling HIS to process health records as a moderator in the relationship of identified constructs and users' compliance behaviour with ISPs. Such experience includes experience with information security incidents, information security training and understanding the consequences of

not complying with the policies relating to the HIS security policies. Benner [66] states that employee's working experience with system environment in the same or similar situations may create competence.
We have divided the working experience of using HIS in two sub-groups: high experience and low experience. Health professionals with working experience of more than five years are classified to the group of higher HIS usage (i.e., high experience users) whilst those with less than five years are classified as lower HIS usage (i.e., low experience users) [67]. Based on the nature of Malaysian HIS, the experiences of health professionals are connected to the system usage. We believe that low experience users are more influenced by management support because most of them are concerned about their reputation in the organization. Meanwhile, employees who have longer experiences using HIS have better knowledge and skills in IS usage[68]. Experienced employees with proper knowledge can reduce the barrier of practicing ISPs, thus increasing compliance behavior. Moreover, experienced employees know the ins and outs of the organization, so trust relationship has been built. Thus, we believe that employees' experience can strongly moderate the relationship between the following constructs (i.e., management support, information security awareness, perceived barrier, self-efficacy and perceived trust) and ISPs compliance behavior; and the following hypothesesare constructed:

H8: The relationship of management support and user's ISPs compliance behavior is stronger in users with low experience of using HIS than high HIS experience.
H9: The relationship of information security awareness: (a) perceived benefit; (b)perceived severity and (c) perceived susceptibility, and user's ISPs compliance behavior is stronger in users with high experience of using HIS than low HIS experience.
H10: The relationship of a perceived barrierand user's ISPs compliance behavior is stronger in users with high experience of using HIS than low HIS experience.
H11: The relationship of a self-efficacy and user's ISPs compliance behavior is stronger in users with high experience of using HIS than low HIS experience.
H12: The relationship of a perceived trust and user's ISPs compliance behavior is stronger in users with high experience of using HIS than low HIS experience.

4.0 RESEARCH METHODOLOGY

4.1 Instruments

A questionnaire is prepared in two languages - English and Bahasa Melayu (i.e., national language). The reasons for translating the questionnaire to the Bahasa Melayu language is to ensure that respondents had a solid understanding of the response statements. It is divided into three sections: Section A captured demographical profiles of the respondents such as age, HIS experience, gender and occupation. Section B assesses health professional perceptions of management support of information security, information security awareness, self-efficacy, barriers and trust of ISPs.

The items are used to measure HISSPC construtsand adapted from previous human behaviour study that relate with policies compliance behaviour. Indicators are used to measure management support and adapted from Aaron [49] for leadership behaviour, Meillier et al. [69] and Ng et al. [32] for information security training and ISPs implementation.

We adapt items which are used to measure information security awareness constructs from several literatures: perceived severity and perceived susceptibility [32], and perceived benefit [70]. Items are used to measure perceived barrier andadapted from Ng et al. [32] while self-efficacies are adapted from Ifinedo[30] and perceived trusts are adapted from Chung and Kwon [59].

Finally, Section C focuses on health professionals' compliance behaviour towards ISPs where the measurement items adapted from Siponen et al. [20]. The constructs in Sections B and C are measured using multiple versions of adapted items (i.e., Appendix A) with 5-point Likert scale (i.e., Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree) [71].

Before we proceed with the survey study, content validity is conducted to test the validity of the questionnaires. *Firstly*, the questionnaire needed to go through the translation process in an attempt to minimise any possible variance due to cultural and linguistic difference [72]. Back translation technique is chosen. In doing so, two bilingual translators competent in both English and Bahasa Melayuare involved in the translation process. *Next*, a pilot study is conducted in which the questionnaire is randomly distributed to 42 respondents, who are then excluded

from the actual respondents in the population. The reliability of the pilot study questionnaire is assessed based on the Cronbach's Alpha (CA) coefficient. In this study, the range of reliability results for each construct in the pilot study is from .713- to .917, which is acceptable [73].

4.2 Data collection

The current study is carried out in collaboration with three government hospitals in Malaysia (i.e., Serdang Hospital, Selayang Hospital and Sungai Buloh Hospital). The samples of the current study are not homogeneous; thus, stratified random sampling is used to determine sample sizes to ensure that an adequate number of subjects are selected from each category of employees at the selected local hospitals. The respondents in this study are employees working as health professionals (e.g., doctors, support staff and health administrators) who are end-users of HIS. The total population from these three hospitals is 7760 employees. If the population size is more than 5000, an adequate sample size will be 400 to 500 [74]. However, considering the size of the total population and the amount of error, which in the current study is to be within 5 percentage points (i.e., with 95 percent certainty), the sample size calculator is used to determine the required sample size [75], which in this case is 367. We calculate the sample size neededfor each hospital and from each category of health professionals using the following formula.

Formula to calculate the sample size needed for each hospital:

$$S = (\text{size of hospital population} / \text{total of population}) * 367 \quad (1)$$

Formula to calculate the sample size needed from each category of health professionals:

$$s1 = (\text{total of employee} / \text{size of hospital population}) * S \quad (2)$$

Table 2: Demographics profiles

	Full n = 454		High Experience n = 226		Low Experience n = 228	
Demographics	**Frequency**	**Percentage**	**Frequency**	**Percentage**	**Frequency**	**Percentage**
Gender						
Male	97	21.40%	54	23.90%	43	18.90%
Female	357	78.60%	172	76.10%	185	81.10%
Ages						
< 40 years	394	86.70%	167	77.50%	227	99.50%
>= 40 years	60	13.20%	59	22.50%	1	0.50%
Hospitals						
Selayang	159	35.00%	88	38.90%	71	31.10%
Sungai Buloh	166	36.60%	78	34.50%	88	69.70%
Serdang	129	28.40%	60	26.50%	69	30.30%
Positions						
Doctors	132	29.00%	63	27.90%	69	30.30%
Support staffs	278	61.30%	136	58.00%	142	62.40%
Health administrators	44	9.70%	27	11.90%	17	7.40%

To avoid any issue of non-response and sampling error, a total of 900 questionnaires are distributed, in which 300 questionnaires are allocated for each hospitals. Finally, 454 questionnaires are returned and validated. Demographic profiles of this study are presented in Table 2.

5.0 ANALYSIS AND FINDINGS

5.1 Analysis tools and method

IBM SPSS statistics 21.0 is employed to screen data in terms of coding, outliers, normality, exploratory factor analysis (EFA) and assessment of common method bias (CMB). Based on the skewness and kurtosis results, research data are considered normal. However, the Partial Least Square-Structural Equation Modeling (PLS-SEM)is applied to test the hypotheses as the premise of the current study is geared towards predictive analysis; the conceptual model of the current study can be categorised as prediction-oriented modelling. In this case, SmartPLS 2.0 is used to test the measurement and structural model of the current study [76]. Bootstrapping with 500 re-samples is performed to obtain the statistical significance of path coefficients using a t-test.

The EFA results showed that all the indicators are used to measure leadership behaviour, ISPs training and implementation and loaded into one factor; namely, management support. Meanwhile, the indicatorsare used to measure other constructs in the research modeland loaded into the constructs that represent the indicators. Using principal component analysis with Varimax rotation, the seven constructs (i.e., management support, perceived severity, perceived benefit, perceived susceptibility, self-efficacy, perceived barrier and perceived trust) are retained, which explained approximately 68% of the total variance (i.e., eigenvalues greater than 1). These seven constructs are used in confirmatory factor analysis (CFA).

Before we proceed with CFA, Harman's single-factor test is conducted to assess the CMB. CMB is defined as "variance that is attributable to the measurement method rather than to the constructs the measure represent" [77, p.289]and could be problematic. The basic assumption of this test is that if a substantial amount of common method variance (CMV) is present, a factor analysis of all the data will result in a single factor accounting for the majority of the covariance in the variables. An unrotated single-factor analysis of all the items resulted in less than 50% percent of the variance. Given that a single factor solution did not emerge and a general factor did not account for most of the variance, CMV is not viewed as a significance threat in this current study [78].

5.2 Measurement model

The measurement model is assessed separately for the full model and each model of the groups. All constructs in the model satisfied the requirements for reliability (i.e., composite reliability [CR] greater than 0.7)and discriminant validity (i.e., average variance extracted [AVE] greater than 0.5 and square root of AVE greater than each correlation coefficient).

$$CR = \frac{(\sum_i)^2 \text{Var } F}{(\sum_i)^2 \text{Var } F + \sum_{ii}}$$

,where $_i$, F, and $_{ii}$, are the factor loading, factor variance, and error variance respectively.

$$AVE = \frac{\sum \lambda_i^2}{\sum \lambda_i^2 + \sum_i \text{Var}\lambda_{\varepsilon i})}$$

,whereλ_i is the component loading of each item to a construct and (ε_i) is 1 - λ_i^2

$$CA = \frac{N - \hat{r}}{1 + (N - 1) - \hat{r}}$$

, where N is the number of items and $\hat{r}$ is the average inter-correlation among items (average of all pearson correlation coefficients between the items)

The collected data have been verified for its reliability by calculating the Cronbach's Alpha (CA). The resulting values are acceptable. The results of the measurement model for each group show that all the seven constructs are valid measures based on their parameter estimates and statistical significances [73]. The formulas are used to calculate CR, AVE and CA [73] as above.

The discriminant validityis tested by examining the squared correlations between the measures of potentially overlapping constructs. The results (i.e., Table 3) show that all diagonal values in bold are higher than the values in its row and column, indicating adequate discriminant validity; this means no overlapping construct exists.

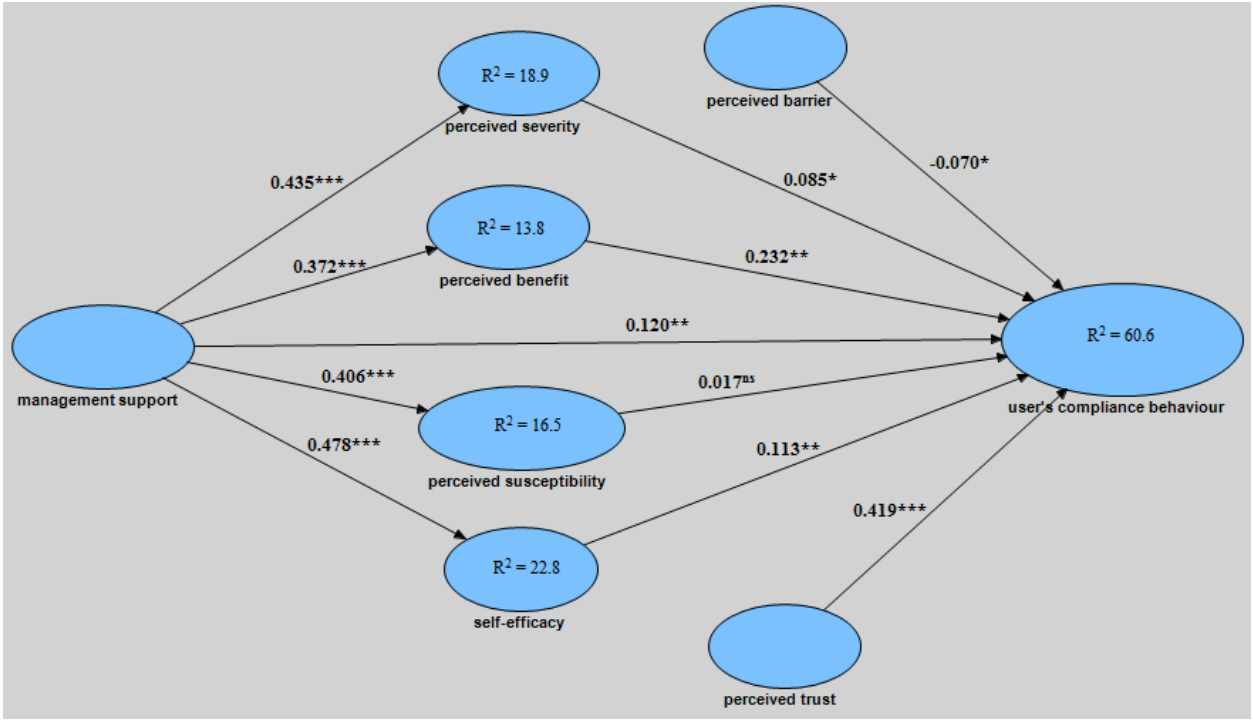
5.3 Structural model

To test the moderating effect of working experience, we estimate three separate models in PLS: the full sample, high experience sub-group and low experience sub-group. The differences across all the three models are tested using test for difference suggested by Chin and Dibbern[79]. To evaluate the structural models' predictive power, we calculate R^2 for user's compliance behaviour with ISPs of HIS. Bootstrapping technique is used to calculate path estimate and t-statistics for the hypothesized relationships. The results suggest that some antecedents influence user's compliance behaviour with ISPs of HIS within each group. The result using PLS are shown in Fig. 2 – IV.

In Fig. 2, the PLS results in the full sample group model is tested without suggesting a moderating effect of working experience. The research hypotheses raised in previous sections are proven in a statistically significant way. Management Support is found to have significant influence on self-efficacy (i.e., $\hat{\beta} = 0.478$***), user's compliance behaviour (i.e., $\hat{\beta} = 0.120$*), perceived severity (i.e., $\hat{\beta} = 0.435$***), perceived susceptibility (i.e., $\hat{\beta} = 0.406$***) and perceived benefit of security-countermeasure (i.e., $\hat{\beta} = 0.372$***). Thus, *H1a-H1c, H2 and H3*are supported. The hypotheses testing also showed the effect of self-efficacy (i.e., $\hat{\beta} = 0.113$*), perceived barrier (i.e., $\hat{\beta} = -0.070$*), perceived severity (i.e., $\beta = 0.085$*), perceived benefit of security-countermeasure (i.e., $\hat{\beta} = 0.232$**) and perceived trust (i.e., $\hat{\beta} = 0.415$***) on user's compliance behaviour towards ISPs are significance, while perceived susceptibility is not significant (i.e., $\hat{\beta} = 0.017$). Overall, it is found that perceived trust is the most significant predictor of HIS's security policies compliance behaviour. These results provide support for *H4a*, *H4c*, *H5*, *H6*and *H7* whereas *H4b*are not supported.

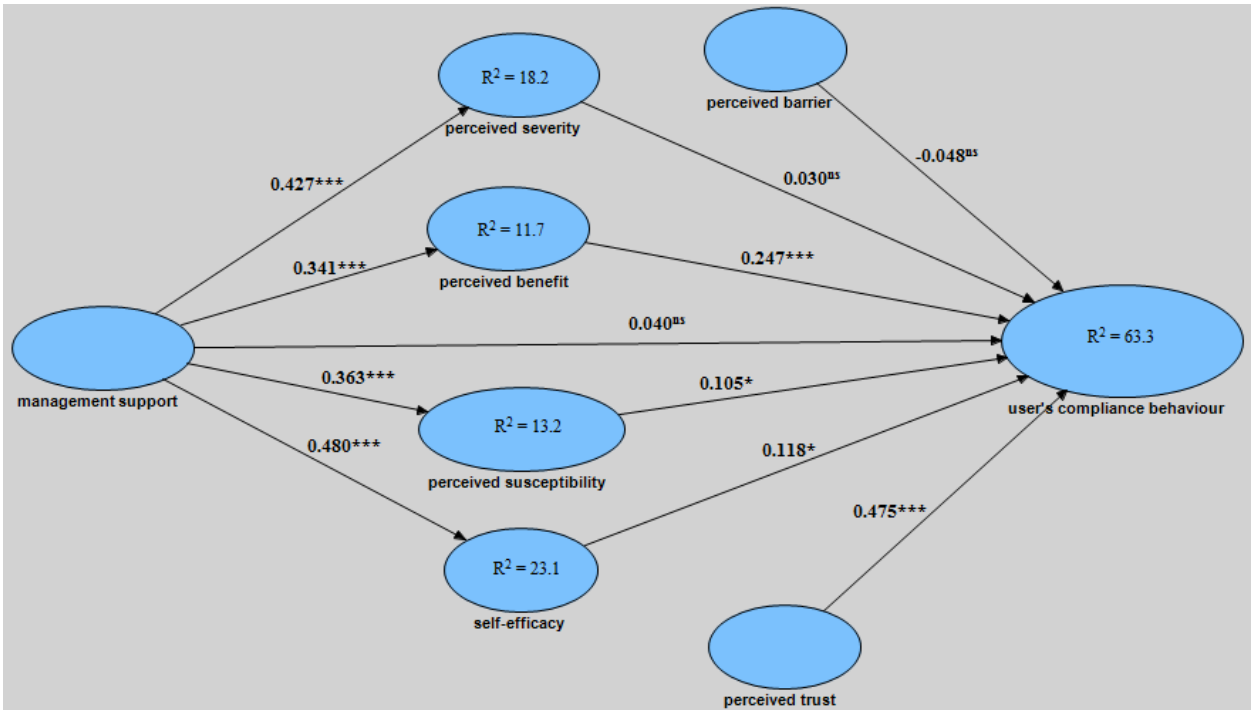
The moderating effect of working experience is presented in Fig. 3 (i.e., high experience) and Fig. 4 (i.e., low experience)for hypotheses H8-H12. Having gained confidence that the measures work appropriately for both sub-groups, the explanatory power of the entire model is tested as well as the predictive power of the independent variables of each sub-group. The explanatory power is examined by looking at squared multiple correlations, R^2 of the main dependent variable. As can be inferred from Fig. 3 and Fig. 4, the variance results of both sub-groups suggest that differences exist across sub-groups. The structural model predicted 3.2% more of the variations in user's compliance behaviour with ISPs in low experience sub-group than in the high experience sub-group. The moderator effectis tested by examining the magnitude of the difference in the standardized parameter estimates between the two groups together with the corresponding t- values that indicate the level of significance. An overview of the statistical comparisons of path results can be inferred from Table 4.

The findings show that management support influences information security awareness and self-efficacy for both sub-groups. Notably, management support strongly influences user's ISPs compliance behavior in low experience subgroup while in high experience sub-group is non-significant. Meanwhile, perceived benefit, perceived trust, and self-efficacyare significance in both sub-groups, but the relationship between perceived benefit and perceived trust, and user's ISPs compliance behaviorisstronger in high experienced user while self-efficacy is stronger in low experienced user.Perceived susceptibility is only significant in the high experience sub-group while perceived severity is significant only in the low experience sub-group. Meanwhile perceived barrier is non-significant in both sub-groups. Perceived trust is significant for both groups.According to Chin and Dibbern[79], the appropriate way to compare the results of different samples is to calculate the t-tests, which is based on standard error (S.E) for the structural paths.



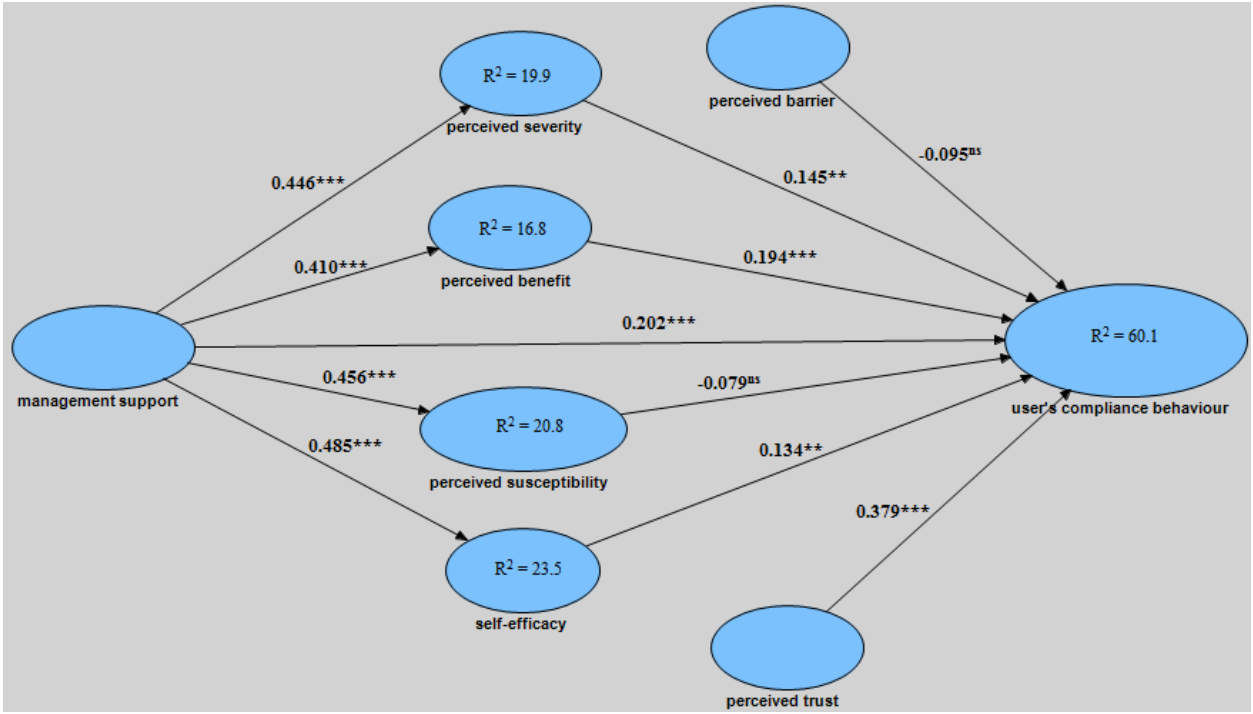
Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Fig. 2: Full Model



Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Fig. 3: High Experience Group Model



Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Fig. 4: Low Experience Group Model

The significance of group differences show that the effect (i.e., path coefficient) of management support on user's compliance behaviour with ISPs is significantly stronger (i.e., t-value = 2.001*) for low experience than for high experience sub-group. Experience also moderates the relationship (i.e., t-value = 1.823*) between perceived susceptibility and user's compliance behaviour with ISPs. Perceived susceptibility has significant effect on UCB in high experience but not for low experience sub-group. Thus, only H8 and H9b are supported, while the other moderating hypotheses are rejected. The overview of the results is presented in Table 4.

In moderation analysis, the R^2 change becomes an important issue as such we will first look at the R^2 change from the main effect model (i.e., Fig. 2: Full model). Using the formula given by [80], the moderating effect analysis results show that the effect size, f^2 for high experience group is 0.07 and low experience group is 0.01. So based on the f^2 of 0.07 for high experience user, we can conclude that the effect size is small as per Chin [81], while f^2 of 0.01 (i.e., low experience group) has no effect. Chin also stated that a low effect size f^2 does not necessarily imply that the underlying moderator effect is negligible.

Table 3: Construct and reliabilityvalidity

Models/Constructs	Cronbach's α	Composite Reliability	AVE	Correlation of constructs							
				MS	PBAR	PBEN	PSEV	PSUS	PTRUST	SE	UCB
Full Model											
MS	0.957	0.961	0.590	**0.768**							
PBAR	0.713	0.837	0.635	0.006	**0.797**						
PBEN	0.895	0.920	0.656	0.372	-0.082	**0.810**					
PSEV	0.797	0.880	0.711	0.435	-0.096	0.528	**0.843**				
PSUS	0.858	0.904	0.703	0.406	-0.056	0.519	0.593	**0.839**			
PTRUST	0.905	0.934	0.779	0.525	-0.122	0.539	0.519	0.469	**0.882**		
SE	0.817	0.879	0.645	0.478	0.213	0.309	0.353	0.291	0.366	**0.803**	
UCB	0.875	0.914	0.727	0.523	-0.125	0.596	0.533	0.469	0.708	0.415	**0.852**
High Experience											
MS	0.959	0.963	0.604	**0.777**							
PBAR	0.739	0.853	0.661	-0.057	**0.813**						
PBEN	0.909	0.929	0.687	0.341	-0.090	**0.829**					
PSEV	0.798	0.880	0.710	0.427	-0.128	0.458	**0.842**				
PSUS	0.834	0.889	0.668	0.363	-0.018	0.429	0.538	**0.817**			
PTRUST	0.916	0.940	0.798	0.511	-0.203	0.512	0.579	0.416	**0.893**		
SE	0.844	0.895	0.680	0.481	0.212	0.271	0.347	0.232	0.341	**0.825**	
UCB	0.907	0.935	0.782	0.477	-0.149	0.599	0.538	0.467	0.733	0.390	**0.884**
Low Experience											
MS	0.954	0.959	0.579	**0.761**							
PBAR	0.674	0.760	0.534	0.074	**0.731**						
PBEN	0.879	0.908	0.624	0.410	-0.077	**0.790**					
PSEV	0.798	0.881	0.712	0.446	-0.061	0.609	**0.844**				
PSUS	0.882	0.919	0.738	0.456	-0.119	0.631	0.651	**0.859**			
PTRUST	0.895	0.927	0.761	0.545	-0.076	0.571	0.457	0.528	**0.872**		
SE	0.786	0.861	0.608	0.485	0.163	0.369	0.369	0.360	0.406	**0.779**	
UCB	0.842	0.894	0.677	0.574	-0.102	0.588	0.530	0.490	0.686	0.467	**0.823**

Note: Diagonal elements in the 'correlation of constructs' matrix are the square root of average variance extracted (AVE). For adequate discriminant validity, diagonal should be greater than corresponding off-diagonal elements.

Legends: MS – management support; PBAR – perceived barrier; PBEN – perceived benefit; PSEV – perceived severity; PSUS – perceived susceptibility; PTRUST – perceived trust; SE – self-efficacy; UCB – user's information security policies compliance behaviour.

Table 4: Statistical comparisons of path coefficients

Hypotheses	Path	High experience sub-group (n = 226)		Low experience sub-group (n = 228)		t-value
		Standard Path Coefficient	Standard Error	Standard Path Coefficient	Standard Error	
H8	MS --> UCB	0.035	0.055	***0.195***	0.058	***2.001** (Accepted)***
H9a	PBEN --> UCB	*0.247*	0.056	*0.195*	0.070	0.581 (Rejected)
H9b	PSEV --> UCB	0.024	0.068	*0.143*	0.068	1.240 (Rejected)
H9c	PSUS --> UCB	***0.105***	0.067	-0.075	0.080	***1.823* (Accepted)***
H10	PBAR --> UCB	-0.060	0.044	-0.085	0.070	0.302 (Rejected)
H11	SE --> UCB	*0.126*	0.072	*0.131*	0.050	0.057 (Rejected)
H12	PTRUST --> UCB	0.468	0.053	*0.378*	0.059	1.137 (Rejected)

Note: Bold and italic values represent the standard path coefficient is significant for each model of the sub-groups. (Significance level of two tailed: t-value => 1.65,*p-value < 0.1; t-value => 1.96, **p-value < 0.05; t-value => 2.58, ***p < 0.01).

6.0 DISCUSSIONS AND IMPLICATIONS

This study might be the first to utilize the multidimensional approach of human-technical interactions via multidisciplinary theories (i.e.,Theory of Planned Behaviour, Health Belief Model, and Trust) to evaluate the relationship between the integrated social-technical values and actions of compliance towards HIS security policies among selected Malaysian health professionals. This study introduced a new human behaviour model, namely, Health Information System Security Policies Compliance Behaviour (HISSPC) by positing the working experience in healthcare environment as a moderating variable in the context of security management, which is largely unknown among scholars to investigate HIS security policies compliance behaviour among Malaysian health professionals.This study tested the research models separately to investigate the moderating effect of health professional's working experience for each group (i.e.,full model, high experience model and low experience model) to explain the impact of management support, information security awareness, perceived barrier, perceived trust and self-efficacy on user's compliance behaviour towards policies related to HIS security.

This study also fills the research gap between different constructs of Management Support and compliance behaviour. Although the role of management has been used extensively to evaluate the links between employees' behaviour and technological effectiveness in the Malaysian culture, none of them has connected managerial support with HIS security effectiveness through compliance behaviour. This study has emphasized the consideration on dual aspects of managerial support (i.e.,leadership behaviour, information system security policies training and implementation) in evaluating the patterns of compliance behaviour among health professionals with different durations of working experience in healthcare environment.

The PLS-SEM analysis for full model group shows that management support influence information security awareness, self-efficacy and user's compliance behaviour towards ISPs. The respondents believed that information security training and awareness programme are important. They also believe that good training and effective security awareness programme can improve their behaviour toward information security, as well as enhance their skill in using information security tools. Thus, Malaysian public hospital management personnel such as hospital directors and hospital information technology (IT) managers play an important role in sorting out problems of human errors before developing any policies related with information security. Moreover, organizations should invest and spend more in information security training and education to maintain information security awareness in hospitals.

Moreover, perceived susceptibility and perceived barrier do not seem to affect user's behaviour towards complying with ISPs for low experience user group, while other HISSPC constructs (i.e., perceived severity, perceived benefit of security-countermeasure, self-efficacy, management support and perceieved trust) are significant. The majority of the respondents from low experience groupdid not find health data to be susceptible to security risks, probably because they are lack of experience and not familiar with security threats. They may also think that current security technologies are able to protect health data. Therefore, it is very important to educate new users about risks of information security threats. Users should be aware of the probability of information security threats that may exist in the organization (i.e., perceived susceptibility), and the consequences of information security threats to the employees and organization (i.e., perceived severity) if the threat exists [82]. In addition, users also must be able to identify information security threats [83], so that they would be able to adjust their action. However, this action is based on their decision, and employees make decisions based on their understanding of the subject [13]. Low experienced users probably also prefer to avoid problems with the management of the hospital due to their carelessness in practising information security behaviour since they are trying to build their career in the organisation. Previous studies suggest that if employees perceive higher levels of penalties for non-compliance with ISPs such as loss of job or heavy fines, their non-compliance behaviour is likely to decrease [20, 84]. Additionally, if employees are not aware of their security actions, it may result in many security incidents [85]. Therefore, the management plays an important role in injecting the right knowledge about information security to all employees by conducting information security training and education, and implementing security awareness programmes or campaigns effectively.

Similar to the low experience users, perceived barrier isalso found to be insignificant for the high experience users. This indicates that the perceived barrier is not an important factor for Malaysian health professionals to comply with

ISPs related with HIS uses, regardless of whether they have a long or lessworking experience in the healthcare sector.Meanwhile, perceived benefit of security-countermeasure and perceived trust significantly affect high experience users'compliance behaviour towards HIS security policies. This indicates that if HIS users are aware of the benefit of security-countermeasure, which is able to prevent security threat, they are more likely to comply with ISPs. The current results are consistent with those reported in previous studies [17, 86]. Meanwhile, trust in an organisation's ISPs is shown to be one of the important factorfor employees to comply and practise security behaviour adequately. Thus, management should document the ISPs efficiently, whereby the documents can be easily understood and applied by all employees in the organisation. Perceived severity and managementsupport are also found to affect ISPs compliance behaviour in users with high experience, however the effects are insignificant. Users with longer working experiences are probably more familiar with the policies and its implementations in the organization, therefore they may not require a stronger support from the management unlike users with low working experience.

Based onmulti-group analysisresults,there are no statistical differences in the standard paths between both sub-groups for perceived severity, perceived benefit, perceived barrier, self-efficacy and perceived trust. However, both groups have a different perspective on management support concerning compliance behaviour of HIS security policies. The comparison between these groups shows that management support is very significant in influencing users with low experience, while the management support is not significant among highly experienced users. Most users with low experience focus on building their reputation; hence, they tend to be more careful and try to avoid any problems with the management. Moreover, new users will probably be sent for security trainings organised by the institutions. This will help them to be aware of any new policies related to HIS that have been implemented in the health institutions. In line with previous studies, management support is found to be important in promoting information security awareness among IS users [16, 24, 27]. On the other hand, comparison between these groups showed that perceived susceptibility significantly influenced users' compliance behaviour toward HIS policies in the highly experienced group and the path is stronger than users with low experience. This indicates that highly experienced users are more aware of the importance of complying with HIS policies to prevent information security threats that can pose serious problems to the health institutions. This is inline with previous studies that reported experienced users who had experience with security incidents to more likely comply with security policies [16, 87].

7.0 CONCLUSION AND LIMITATIONS

Complexity of issues between HIS and sustainability of compliance behaviour aredealt with the integration between perceptions of health professionals on the HIS security policies and duration of working experience in healthcare environment. The full model tested without a moderating effect of working experience show that all the factors except perceived susceptibility significantly affect users' compliance behaviour towards ISPs. This study found significant differences between low and high experiencegroup whereby management support and perceived susceptibility influence their compliant behaviour towards ISPs. Users with higher working experience have higher absorptive capacity to deal with innovation and catch up with the latest development of advanced security tools to reduce the expected risks of security incidents compared to users with little working experience.

Additionally, the statistical test results of the current study revealed several practical implications. *Firstly*, the health institutions should consider health professionals' experience in using HIS and try to understand employees' particular motives in complying with HIS policies. *Secondly*, management of health institutions such as hospital directors and hospital IT managers play an important role in sorting out problemsofhuman errors before developing ISPs; thus, they should ensure all employees, both new and old, are given information security training in view of the fact that people tend to forget what they have learnt. *Moreover*, the training should be conducted regularly. *Next*, documenting and implementing security policies and procedures are important. Thus, information security guidelines should be clearly written and easy to understand by all employees. *Finally*, information security awareness campaigns should be promoted to ensure that all employees do not forget about their responsibility to comply with ISPs and to keep abreast with the latest security threats.

We suggest that future research should investigate the impact of other moderating factors, such as perceived trust and IS skills. We also recommend the use of a different kind of measurement to measure HIS experience instead of a measure based on number of working years.

In conclusion, the current research findings are believed to contribute to human behaviour studies related to organisations' ISPs compliance behaviour among employees and are beneficial to policy makers in improving organisations' strategic plans of information security, especially in the healthcare sector.

ACKNOWLEDGEMENT

Our thanks and appreciation goes to all of the health professionals who participated in the current study. We would also like to thank the Ministry of Health (MOH) for the permission granted to conduct the survey at the public hospitals and our thanks also goes to Ministry of Higher Education (MOHE) for the study scholarship. Lastly, gratitude is also extended to University of Malaya for the support provided (RP028A-14AET).

APPENDIX A: Items used to measure independent variables and dependent variable

No	Item's Code	Items	Source
Independent Variables			
1) Management support: Leadership Behaviour			
1	MS01	Leader always seek for improvements related to information security policies.	[49]
2	MS02	Leader takes serious action on those who do not comply with information security policies.	
3	MS03	Leader always values the adoption of practicing adequate information security behaviour.	
2) Management support: Information Security Training & ISPs Implementation			
4	MS04	The management always provides specific training on information security regularly.	[69]
5	MS05	The management encourages me to attend any information security training.	
6	MS06	The information security training organizes by the management is complete.	
7	MS07	The information security training organizes by the management is effective.	
8	MS08	The management documents information security policies efficiently where I can understand it easily.	
9	MS09	Information security policies are easy to be accessed in my organization.	
10	MS10	The management updates me on changes related to information security policies.	[32]
11	MS11	There exists a clear structure for disciplinary action in case of non-compliance with organization's information security policy.	[69]
12	MS12	The management considers my job performance will be improved if I adopt information security behaviour adequately.	
13	MS13	Information security policies in my organization help me to understand how to behave appropriately towards matters related to information security.	
14	MS14	Information security articles or newsletters are distributed to all employees in my organization.	[32]
15	MS15	Information security threats are always alerted to all employees through messages/emails in my organization.	
16	MS16	Any changes related to information security policies will always be alerted to all employees through messages/emails in my organization.	
17	MS17	The management organises ingoing information security campaign to increase user's security awareness.	[69]
3) Self-Efficacy			

No	Item's Code	Items	Source
18	SE01	I have the necessary skills to recognize many types of information security violations (eg. Didn't change password, suspicious email and didn't update anti-virus regularly, etc).	[30]
19	SE02	I have the necessary skills to protect my organization's data from information security violations.	
20	SE03	I have the necessary skills to use information security countermeasure if someone tells me what to do as I go along.	
21	SE04	I have the necessary skills to implement the available preventive measures to avoid information security threat.	
4) Perceived Severity			
22	SEV01	If I do not follow information security policy the penalty will be severe.	[34]
23	SEV02	Failure to adopt information security behaviour will jeopardise my career.	
24	SEV03	Failure to adopt information security behaviour will harm my organization's data.	
5) Perceived Susceptibility			
25	SUS01	I am aware that if I did not adopt information security behaviour adequately will cause security incidents.	[32]
26	SUS02	I am aware that if I'm not complying with information security policies in my organization is a serious problem.	
27	SUS03	I am aware that if I am not complying with information security policies, my organization could be subjected to a serious information security threat.	
28	SUS04	I am aware that if organizational data being stolen by unauthorised user is a serious problem.	
6) Perceived Benefit			
29	BEN01	I am aware that information security countermeasure is effective for protecting my organization's data.	[75]
30	BEN02	I am aware that using strong password is effective for avoiding unauthorised access.	
31	BEN03	I am aware that changing password regularly is effective for avoiding unauthorised access.	
32	BEN04	I am aware that using anti-virus regularly is effective for protecting my computer.	
33	BEN05	I am aware that update anti-virus regularly is effective for protecting my computer.	
34	BEN06	I am aware that scanning files and devices before using them is effective for protecting my computer.	
7) Perceived Barrier			
35	BAR01	It is difficult to understand my organization's information security policies.	[32]
36	BAR02	Having to learn how to adopt information security behaviour would imply a significant loss of my time such as scanning files.	
37	BAR03	Adopting information security behaviour is inconvenient.	
8) Perceived Trust			
38	TRUST01	I feel confident understanding the information security policies in my organization.	[59]
39	TRUST02	I feel confident when it comes to implementing information security policies in my organization.	
40	TRUST03	I feel confident practicing information security policies in my organization.	
41	TRUST04	I feel confident with the information security policies in my organization.	
Dependent Variable			
1) User's Compliance Behaviour			
42	UCB01	I comply with information security policies when performing my daily works.	[20]
43	UCB02	I practice recommended information security behaviour as much as possible.	
44	UCB03	I always recommend others to comply with information security policies.	
45	UCB04	I assist others in complying with information security policies.	

REFERENCES

[1] C. Posey, *et al.*, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Information & Management,* vol. 51, pp. 551-567, 2014.

[2] H.-S. Rhee, *et al.*, "Unrealistic optimism on information security management," *Computers & Security,* vol. 31, pp. 221-232, 2012.

[3] P. A. H. Williams, "In a 'trusting' environment, everyone is responsible for information security," *Information Security Technical Report,* vol. 13, pp. 207-215, 2008.

[4] G.N.Samy, *et al.*, "Security threats categories in healthcare information systems," *Health Information Journal,* vol. 16, pp. 201-209, 2010.

[5] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," *Information Security Technical Report,* vol. 14, pp. 186-196, 2009.

[6] D. Liginlal, *et al.*, "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management," *Computers & Security,* vol. 28, pp. 215-228, 2009.

[7] K. Renaud, "Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?," *Security & Privacy, IEEE,* vol. 10, pp. 57-63, 2012.

[8] C. Vroom and R. von Solms, "Towards information security behavioural compliance," *Computers & Security,* vol. 23, pp. 191-198, 2004.

[9] R. N. Keers, *et al.*, "Causes of Medication Administration Errors in Hospitals: a Systematic Review of Quantitative and Qualitative Evidence," *Drug Safety,* vol. 36, pp. 1045-1067, 2013.

[10] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Applied Ergonomics,* vol. 38, pp. 143-154, 2007.

[11] C. C. Wood and W. W. Banks Jr, "Human error: an overlooked but significant information security problem," *Computers & Security,* vol. 12, pp. 51-60, 1993.

[12] K. J. Knapp, *et al.*, "Information security policy: An organizational-level process model," *Computers & Security,* vol. 28, pp. 493-508, 2009.

[13] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & Security,* vol. 25, pp. 289-296, 2006.

[14] M. Siponen, *et al.*, "Employees' adherence to information security policies: An exploratory field study," *Information & Management,* vol. 51, pp. 217-224, 2014.

[15] M. Eminağaoğlu, *et al.*, "The positive outcomes of information security awareness training in companies – A case study," *Information Security Technical Report,* vol. 14, pp. 223-229, 2009.

[16] A. Al-Omari, *et al.*, "Information security policy compliance: The role of information security awareness," Seattle, WA, 2012, pp. 1633-1640.

[17] J. M. Hagen, *et al.*, "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security,* vol. 16, pp. 377-397, 2008.

[18] Y. Rezgui and A. Marks, "Information security awareness in higher education: an exploratory study," *Computers & Security*, vol. 27, pp. 241-253, 2008.

[19] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, pp. 432-445, 2010.

[20] M. Siponen, *et al.*, "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, vol. 43, pp. 64-71, 2010.

[21] A. Vance, *et al.*, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, pp. 190-198, 2012.

[22] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, pp. 106-125, 2009.

[23] H. Li, *et al.*, "Understanding compliance with internet use policy from the perspective of rational choice theory," *Decision Support Systems*, vol. 48, pp. 635-645, 2010.

[24] J. W. Brady, "An investigation of factors that affect HIPAA security compliance in academic medical centers," Ph.D. 3411810, Nova Southeastern University, United States -- Florida, 2010.

[25] C. Kogler, *et al.*, "Trust and power as determinants of tax compliance: testing the assumptions of the slippery slope framework in Austria, Hungary, Romania and Russia," *Journal of Economic Psychology*, vol. 34, pp. 169-180, 2013.

[26] D. Van Maele and M. Van Houtte, "The role of teacher and faculty trust in forming teachers' job satisfaction: Do years of experience make a difference?," *Teaching and Teacher Education*, vol. 28, pp. 879-889, 2012.

[27] M. Warkentin, *et al.*, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, vol. 20, pp. 267-284, 2011.

[28] B. Bulgurcu, *et al.*, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quaterly*, vol. 34, pp. 523-548, September 2010.

[29] A. Rapp, *et al.*, "The impact of knowledge and empowerment on working smart and working hard: The moderating role of experience," *International Journal of Research in Marketing*, vol. 23, pp. 279-293, 2006.

[30] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, pp. 83-95, 2012.

[31] D. W. Straub, "Effective IS security: An empirical study," *Information Systems Research*, vol. 1, pp. 255-276, 1990.

[32] B.-Y. Ng, *et al.*, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, pp. 815-825, 2009.

[33] T. P. Ross, *et al.*, "The bicycle helmet attitudes scale: using the Health Belief Model to predict helmet use among undergraduates," *Journal of Ameican College Health*, vol. 59, pp. 29-36, 2010.

[34] E. E. Bonar and H. Rosenberg, "Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies," *Addictive Behaviors*, vol. 36, pp. 1038-1044, 2011.

[35] C. L. Bylund, *et al.*, "Using the Extended Health Belief Model to understand siblings' perceptions of risk for hereditary hemochromatosis," *Patient Education and Counseling,* vol. 82, pp. 36-41, 2011.

[36] M. E. Buglar, *et al.*, "The role of self-efficacy in dental patients' brushing and flossing: Testing an extended Health Belief Model," *Patient Education and Counseling,* vol. 78, pp. 269-272, 2010.

[37] C. Liao, *et al.*, "Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model," *Computers in Human Behavior,* vol. 23, pp. 2804-2822, 2007.

[38] Y. Lu, *et al.*, "Exploring chinese users' acceptance of instant messaging using theory of planned behavior, the technology acceptance model, and the flow theory," *Computers in Human Behavior,* vol. 25, pp. 29-39, 2009.

[39] D. R. Poulter, *et al.*, "An application of the theory TPB to truck driving behaviour and compliance with regulations," *Accident Analysis & Prevention,* vol. 40, pp. 2058-2064, 2008.

[40] E. M. Welsh, *et al.*, "Measuring perceived barriers to healthful eating in obese, treatment-seeking adults," *Journal of Nutrition Education and Behavior,* pp. 1-6, 2011.

[41] E. Huang and M. H. Chuang, "Extending the theory of planned behavior as a model to explain post-merger employee behavior of IS use," *Computers in Human Behavior,* vol. 23, pp. 240-257, 18 November 2004 2007.

[42] D.-L. Huang, *et al.*, "Factors affecting perception of information security and their impacts on IT adoption and security practices," *International Journal of Human-Computer Studies,* vol. 69, pp. 870-883, 2011.

[43] L. B. Huang, V. Balakrishnan, R.G. Raj, "Improving the relevancy of document search using the multi-term adjacency keyword-order model." Malaysian Journal of Computer Science, Vol. 25, No. 1, 2012, pp. 1-10.

[44] I. M. Y. Woon and A. Kankanhalli, "Investigation of IS professionals' intention to practise secure development of applications," *International Journal of Human-Computer Studies,* vol. 65, pp. 29-41, 2007.

[45] P. Puhakainen, "A design theory for information security awarenss," ed. Oulu, Finland, 2006.

[46] I. Koskosas, *et al.*, "Examining the linkage between information security and end-user trust," *International Journal of Computer Science & Information Security,* vol. 9, pp. 21-31, 2011.

[47] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security,* vol. 29, pp. 196-207, 2010.

[48] J. M. Burns, "Leadership," in *New York: Harper and Row*, ed, 1978.

[49] G. A. Aaron. (2006, Retrieved August 26, 2007.). Transformational and transactional leadership: Association with attitudes toward evidence-based practice. *Psychiatric Services57(8),* 1162-1169.

[50] M.-C. Lo, *et al.*, "Does transformational leadership style foster commitment to change? The case of higher education in Malaysia," *Social and Behavioral Science,* vol. 2, pp. 5384-5388, 2010.

[51] N. Martin and J. Rice, "Cybercrime: Understanding and addressing the concerns of stakeholders," *Computers & Security,* 2001.

[52] M. Workman, *et al.*, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior,* vol. 24, pp. 2799-2816, 2008.

[53] L. Younghwa, "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective," *Decision Support Systems,* vol. 50, pp. 361-369, 2011.

[54] Y. J. Lee, *et al.*, "Profit-maximizing firm investments in customer information security," *Decision Support Systems,* vol. 51, pp. 904-920, 2011.

[55] A. C. Johnston and M. Warkentin, "Information privacy compliance in the healthcare industry," *Information Management & Computer Security,* vol. 16, pp. 5-19, 2008.

[56] M. Chan, *et al.*, "Perceptions of information security in the workplace: linking information security climate to compliant behavior," *Journal of Information Privacy and Security,* vol. 1, 2005.

[57] M. I. Beas and M. Salanova, "Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers," *Computers in Human Behavior,* vol. 22, pp. 1043-1058, 2006.

[58] G. Torkzadeh and T. P. Van Dyke, "Effects of training on Internet self-efficacy and computer user attitudes," *Computers in Human Behavior,* vol. 18, pp. 479-494, 2002.

[59] N. Chung and S. J. Kwon, "Effect of trust level on mobile banking satisfaction: A multi-group analysis of information system success instruments," *Behaviour & Information Technology,* vol. 28, pp. 549-562, 2009.

[60] D. J. Kim, *et al.*, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems,* vol. 44, pp. 544-564, 2008.

[61] C. Kim, *et al.*, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electronic Commerce Research and Applications,* vol. 9, pp. 84-95, 2010.

[62] J. Dumortier and N. Vandezande, "Trust in the proposed EU regulation on trust services," *Computer Law & Security Review,* vol. 28, pp. 568-576, 2012.

[63] A. Shen, *et al.*, "How social influence affects we-intention to use instant messaging: The moderating effect of usage experience," *Information Systems Frontiers,* vol. 13, pp. 157-169, 2011.

[64] Á. Crespo, *et al.*, "Influence of Users' Perceived Compatibility and Their Prior Experience on B2C e-Commerce Acceptance," in *Electronic Business and Marketing*. vol. 484, T. Matsuo and R. Colomo-Palacios, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 103-123.

[65] K.-M. Lin, "e-Learning continuance intention: Moderating effects of user e-learning experience," *Computers & Education,* vol. 56, pp. 515-526, 2011.

[66] P. Benner, *From novice to expert: Excellence and power in clinical nursing practice*. Menlo Park, CA: Addison-Wesley, 1984.

[67] M. D. McHugh and E. T. Lake, "Understanding Clinical Expertise: Nurse Education, Experience, and the Hospital Context," *National Institute of Health (NIH) Public Access,* vol. 33, pp. 276–287, 2010.

[68] W. Rodgers, *et al.*, "The moderating effect of on-line experience on the antecedents and consequences of on-line satisfaction " *Psychology & Marketing,* vol. 22, pp. 313-331, 2005.

[69] L. K. Meillier, *et al.*, "Cues to action in the process of changing lifestyle," *Patient Education and Counseling,* vol. 30, pp. 37-51, 1997.

[70] J. D. Arcy, *et al.*, "User awareness of security countermeasures and its impact on information system misuse: a deterrence approach," *Information Systems Research,* vol. 0, pp. 79-98, 2009.

[71] R. Likert, "A technique for the measurement of attitudes," *Archives of psychology,* 1932.

[72] I. M. Saidon, "Moral Disengagement in Manufacturing: A Malaysian Study of Antecedents and Outcomes," Doctor of Philosophy Thesis, Curtin Graduate School of Business, Curtin University, Curtin, 2012.

[73] J. F. Hair, *et al.*, *Multivariate Data Analysis: A Global Perspective*, 7th ed. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2010.

[74] P. Singh, *et al.*, *A comprehensive guide to writing a research proposal*: Venton Publishing, 2006.

[75] R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities.," *Educational and Psychological Measurement*, vol. 30, pp. 607-610, 1970.

[76] C. M. Ringle, *et al.* (2005, *SmartPLS 2.0 (M3) Beta*. Available: http://www.smartpls.de

[77] P. M. Podsakoff, *et al.*, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology*, vol. 88, pp. 879-903, 2003.

[78] P. M. Podsakoff and D. W. Organ, "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management*, vol. 12, pp. 531-544, 1986.

[79] W. W. Chin and J. Dibbern, "An introduction to a permutation based precedure for multi-group PLS analysis: results of tests of differencces on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA," in *Handbook of Partial Least Squares: concepts, methods and applications*, V. E. Vinzi, *et al.*, Eds., ed Berlin: Springer, 2010.

[80] J. F. J. Hair, *et al.*, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*: SAGE, 2014.

[81] W. W. Chin, "The partial least squares approach to structural equation modelling," in *Modern methods for business research*, G. A. Marcoulides, Ed., ed Mahwah NJ: Lawrence Erlbaum, 1998.

[82] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior*, vol. 28, pp. 2366-2375, 2012.

[83] K.-L. Thomson and R. von Solms, "Towards an Information Security Competence Maturity Model," *Computer Fraud & Security*, vol. 2006, pp. 11-15, 2006.

[84] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, pp. 154-165, 2009.

[85] L. Cheng, *et al.*, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security*, vol. 39, Part B, pp. 447-459, 2013.

[86] A. Hovav and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Information & Management*, vol. 49, pp. 99-110, 2012.

[87] E. Albrechtsen and J. Hovden, "The information security digital divide between information security managers and users," *Computers & Security*, vol. 28, pp. 476-490, 2009.