Journal of
Health & Medical Informatics

Humaidi and Balakrishnan, J Health Med Inform 2013, 4:2
DOI: 10.4172/2157-7420.1000123

Open Access

Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security

Norshima Humaidi[1,2]* and Vimala Balakrishnan[2]

[1]*Faculty of Business and Management, University of Technology MARA, Malaysia*
[2]*Faculty of Computer Science and Information Technology, University of Malaya, Malaysia*

Abstract

One of the main problems in information security was human error due to improper human behaviour. Therefore, this preliminary study was conducted with aims to identify possible factors that can affect user's compliance behaviour towards information security in terms of two aspects: management support and security technology. Two theories were integrated for development of research framework: I) Theory of Planned Behaviour; II) Theory of Acceptance Model. The respondents of this study were the health professionals and IT officers whereby 42 questionnaires were obtained and verified. Exploratory Factor Analysis (EFA) results revealed that the six factors were obtained: Transactional_Leadership_Style, Transformational_Leadership_Style, ISP_Training_Support, PU_Security, PU_Security-Countermeasure and PEOU_ISPs. The higher loadings signalled the correlations of the indicated items with the factors on which they were loaded with each of the correspondence factors achieving score of alpha value above 0.80. According to the descriptive analysis, most of the respondents are agreed with all the indicated factors. The preliminary study facilitates researcher in developing new model that integrates TPB and TAM that can be used to increase knowledge of user's compliance behaviour towards health information system's security.

Keywords: Information security compliance behaviour; Exploratory factor analysis; Management support; Security technology; Information security effectiveness

Introduction

Health Information System (HIS) has been implemented in Malaysia since late 1990s. Since then, HIS is utilized in many government hospitals especially those that are located in Lembah Klang, Kuala Lumpur such as Selayang Hospital, Sungai Buloh Hospital, Serdang Hospital, etc. HIS is an integration of several hospitals' information system to manage administration works, patients and clinical records. HIS can be accessed through Internet where the data can be delivered, stored and processed automatically. Besides, being on the Internet also means that the system is vulnerable to inappropriate use [1]. Health data is extremely sensitive, therefore they require high protection and information security must be carefully watched as it plays an important role to protect the data from being stolen or harmed. Information security can be defined as the protection of information systems from unauthorised access and information threat [2].

Previous studies have stated that external threat is not a major issue in information security because many organizations have implemented advanced security technologies such as smart card and biometrics [3,4]. Until recently, the main critical information security issue identified is internal threat, where is caused by internal factors, mainly the employees' poor users' behaviour such as carelessness, user errors and omission [4]. Many studies have found that the employees of an organization could be the real culprit of most security breaches whether it was done intentionally or unintentionally [3,5]. This notion is supported by Boujettif and Wang [6] who reported that 80% of security incidents in organizations are due to internal threats. In Malaysia, human error is one of major internal threat towards implementation of HIS [7]. Hence, the preliminary study aims to investigate possible factors that will bring forth some effect to the HIS security effectiveness by focusing on the user's compliance behaviour in information security. To be specific, the preliminary study explores user's compliance behaviour in information security by focusing on two aspects that is, management support and security technology. Each aspect was containing several possible factors that tested in factor analysis taken from previous studies [8-12].

The rest of the paper is presented as follows: the next section reviewed several theories related with human behaviour. The third section presents the research framework and discusses the integration theories that were adapted to develop research framework while fourth discusses the research design used in this study. The analysis results of the study are presented in the fifth section. The discussions of the findings are outlined in the sixth section. Finally, the conclusion was the last section.

The Review of Theories

Several theories were reviewed in order to find the right theory to be adapted and then further developed into a new research framework. Previous literatures revealed some theories to investigate users' behaviour towards information system (IS) technology such as the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), and Theory of Planned Behaviour (TPB). However, with a few exceptions, not many have been applied to information security studies [13].

TAM is adapted from TRA and applied in many studies to investigate users' intention behaviour to use IS. TAM is based on two fundamental beliefs: perceived usefulness (PU) and perceived ease of use (PEOU) [11,14], where these two factors have proven as a significant predictor on users' intention behaviour [15]. On the other hand, another theory that has been applied extensively to examine

***Corresponding author:** Norshima Humaidi, Faculty of Business and Management, University of Technology MARA, Malaysia, Tel: +60196421428; E-mail: norshima24@yahoo.com

Received October 18, 2012; **Accepted** January 16, 2013; **Published** January 21, 2013

Citation: Humaidi N, Balakrishnan V (2013) Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. J Health Med Inform 4: 123. doi:10.4172/2157-7420.1000123

user's acceptance towards information system is TPB which is designed to predict human behaviour and postulates that belief affect attitudes, subjective norms and perceived behavioural control [8].

Leach [4] described that human behaviour can be influenced by two group of factors. The first group describes what user understands of what behaviours are expected by others employees and the second group describes about user's willingness to constrain their behaviour to stay within accepted norms based what their belief. This is similar with Social Cognitive Theory (SCT) where the theory explains personal factors and environmental factors which can affect human behaviour. Furthermore, the theory describes that human expectations, belief, emotional benefits and cognitive competencies are developed and modified by social influences that convey information and activate emotional reactions through modelling, instruction and social persuasion [16]. Personal factors such as age, race, sex, and etc can also influence human to evoke different reactions from their social environment [2].

Other theories that are adapted to investigate user's compliance behaviour towards information security are Protection Motivation Theory (PMT), Health Belief Models (HBM), Technology Threat Avoidance Theory (TTAT) and General Deterrence Theory (GDT). PMT is a theory that "explains how people change their health attitude and behaviours in response to health risk message" [17]. For example, if a threat is perceived by people as fearful, then they would prevent the possible threat. PMT was applied successfully in over 30 different domains such as cancer [18], anti-drug abuse [19], and online harassment behaviour [20]. The latter study found that most of the factors such as perceived severity, self efficacy and perceived susceptibility are significantly influenced users to practice security behaviour.

On the other hand, HBM was widely used in health behaviour studies such as drug [21], cancer [22], and dental [23], among others. HBM predicts that if people believe about specific illnesses and know how to prevent the illnesses, they will be more cautious and will practice recommended health behaviour [24]. HBM suggests that individuals determine the feasibility, benefits and cost related to an intervention or behaviour change based on the following factors: perceived susceptibility (similar to perceived vulnerability), perceived benefits, perceive barriers, cue to action, self-efficacy, and perceived severity. Majority of previous studies indicated that most of these factors influence human behaviour.

TTAT is a theory proposed by Liang and Xue [25] has widely been used in IS studies where this theory explains the importance of understanding information technology threat avoidance behaviour of users. The theory suggests that perceived effectiveness, perceived cost and self efficacy constructs can influenced user's information technology threat awareness. Meanwhile, GDT focuses on deterrence or sanctions against deviant behaviour and suggests that when punishment towards deviant behaviour is high and the sanction is severe, potential criminals will be deterred from perpetration illegal acts [26]. Previous literatures have many integrates GDT and PMT in computer security study [27,28].

Though many theories exist, the current study is based on two main technology acceptance models, namely TAM and TPB. These two theories will be further elaborated in the following section. The reviews above also revealed that not many studies have focused on management support and security technology. The current study aims to fill in this gap by exploring and identifying all the possible factors that might influence users' behaviour towards information security based on two aspects: (i) management support and (ii) security technology. The study aims to achieve this by developing a framework that integrates some of the factors from TPB and TAM.

The Research Model

The research model was developed based on the integrations of TAM and TPB where those expected factors under the theories can be grouped under management support and security technology that is explained into detail in the next sections. Management support refers to the commitment from the top management to protect information as a critical security component [29]. Meanwhile, security technology refers to the security mechanisms used to protect the IS such as firewall, user's authentication, encryption and etc.

The integrated research framework comprised six independent variables (transactional leadership style, transformational leadership style, information security policy training support, perceived usefulness of security, perceived usefulness of security-countermeasure and perceived ease of use of ISPs) and user's information security compliance behaviour as independent variable as shown in figure 1. The details about the framework were explained in next section. Definition of each of the independent variables used in this study was stated as shown in table 1.

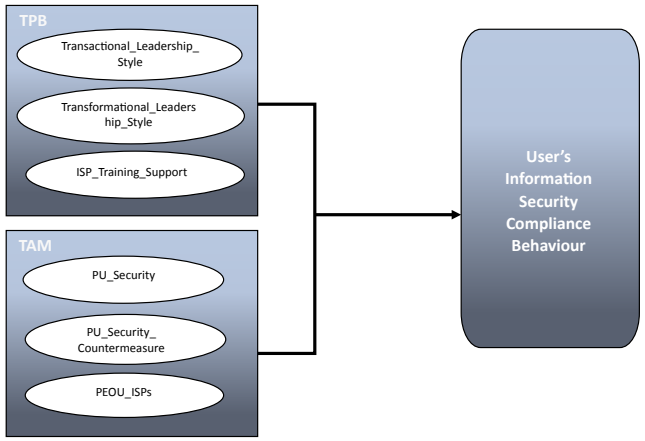

Figure 1: The Integrated Research Framework.

Operational Variable	Definition	Source
Transactional_Leadership_Style	Leader's behaviour that strictly controls how the system is implemented in the organization.	[27]
Transformational_Leadership_Style	Leader's behaviour that are engaged with their team members and motivate them.	[28]
ISP_Training_Support	Programs to impart organization's ISPs.	[29]
PU_Security	Users' belief on usefulness of security that is able to protect data against unauthorized access.	Self definition
PU_Security-Countermeasure	Users' belief on usefulness of security countermeasure to minimize risks that are related to IS threats.	Self definition
PEOU_ISPs	Users' belief that ISP is easy to use, understand and follow.	Self definition

Table 1: Operational Definition of Variables.

Theory of planned behaviour

TPB is designed to predict human behaviour and postulates that belief affect attitudes, subjective norms and perceived behavioural control [8]. Attitude is defined as how users convey positive or negative feelings towards something [30]. Subjective Norms (SN) is defined as users perception of others opinions [8] which are opinion by top management and colleagues. User's behaviour in the organization can be influences by their superior and their colleagues because people tend to follow what other people do or what they have been told either positively or negatively [4]. Meanwhile, Perceived Behavioural Control (PCB) can be described as users perception on his/her ability [30] which can be increased through education and training provided by their management. Recent studies on user's compliance behaviour towards ISPs have adapted TPB [12,31]. Most of their findings have shown that SN and PCB constructs have a significant effect on users' intention to comply with ISP. The same finding also have found by other literatures [32,33] where SN and PCB is strongly significant. Therefore, it is important that management should create adequate security culture among their workers in the organization. This can be done through ongoing security awareness campaign and training [34].

Management plays an important role to encourage positive users' behaviour towards the use of IS [35,36]. Top management must possess definite knowledge on the importance of information security to create an organizational environment that is conducive to achieving the security goals. Studies have suggested that if the employers can provide a set of clear security guidelines and strictly monitor their employees, information security compliances will also increase [27]. The fact is that the common reasons cited for the weak implementation of ISPs in organizations is often caused by the lack of management support in playing their role as they ought to, lack of authority, and lack of understanding of the importance of information security [37]. Therefore, it is essential that the top management plays their role firmly to ensure the effectiveness of information system's security through the implementation of ISP and providing sufficient information security training.

This study identified superior behaviour as style of leadership which is focusing on how leader monitoring and controlling their employees to ensure that they will comply with ISPs. Leadership is defined as the process to influence others to follow rules and procedures to achieve objectives and leadership style refers to the characteristics of the leader to monitor and control their followers [10,38]. The study focuses on two styles of leadership: transformational leadership style and transactional leadership style. Leaders who are engaged with their team members and motivate them is said to have the characteristics of a transformational leader [10], whereas, a transactional leader is one who operates within the existing system or culture and strictly controls how the system is implemented in the organization [9]. Many leadership studies have shown that both of leadership styles significantly influences employee's work performance [39,40]. Strong leadership is required to guide users in making the right decision and to comply with information security policies.

Besides monitoring and controlling employees, management must consider and aware on employee's information security skill where this can be achieved through information security training. Information security training is a program which aims to introduce and provide information about the importance of information system's security and it is able to increase user's skill and understanding towards information security as mentioned in PCB. The effectiveness of information system's security can be achieved by conducting security trainings as training is one of the methods to deliver organization's ISPs [41,42]. Well managed security training can educate employees to comply with ISPs, and therefore, management must ensure that security trainings in their organizations are conducted efficiently.

Technology acceptance model

TAM is based on two fundamental beliefs: perceived usefulness and perceived ease of use [11,14,43]. PU is defined as users believe on the use of the technology will able to enhance their job performance [11]. Meanwhile, PEOU is defined as how users believe that using a particular system will reduced their effort and time [11]. TAM is widely used in study related with e-commerce system [44] and e-learning system [45]. Previous studies have shown that PU and PEOU is contributes to user's behaviour towards IS acceptance [15,44,45].

Based on previous studies which is adapted TAM, researcher concludes that users will have intention to adopt the technology if information system is useful, easy to use and they feel that the technology able to increase their work performance. Security technology is an important element in IS development and thus, it can be one of the factor that can influences users to comply with organization's ISPs. Security technology is a method that can prevent information security threat either internally or externally. Many organizations have invested a huge amount of money to implement the IS security using advanced technological tools such as smartcards and biometrics. However, these tools are only good in preventing the external threat but failed in dealing with the internal threat [46]. Besides, 'passwords' as one of the commonly used method is also well known with its flaw due to users' behaviour [47]. For example, many users fail to use strong passwords, resulting in a low security protection. Many employees also hardly update their anti-virus software or scan their computers regularly. Workman et al. [48] stated that most employees feel that security technology is tedious and time-consuming. Therefore, they usually fail to comply with the ISPs and as a result, increase the vulnerability of the organization's data.

Human behaviour always plays an important role to ensure that organization's information can be protected and secured [49]. When organization implements security technology, they must consider on users' perspective. Sometime technology is so complicated and this make users ignore and did not used it properly. If users feel that information security is easy to understand, then they will be encouraged to behave appropriately towards information security. Therefore, based on the concept of TAM, security technology should be useful and easy.

Research Design

Instrument development

A questionnaire adapted from Aarons [38], Martin and Rice [42], Egea and Gonzalez [14], and Ifinedo [12] was developed to collect the data in this study. The questionnaire was prepared in dual languages, that is English and Bahasa Melayu (national language). It was divided into four sections: Section A consists of demographic questions such as age, experience, gender and occupation. Section B assessed users' perceptions on management support, section C assessed users' perceptions on security technology and finally, section D focused on user's information security compliance behaviour. All the items in sections B, C and D were measured using 5-point Likert-type scale, with anchors ranging from 1 (strongly disagree) to 5 (strongly agree). These measurement items are presented in table 2. Measurement items for PU_Security and PU_Security-countermeasure were self-developed based on TAM concept. There were a total of 29 measurement items.

Variable	Item Text	Adapted From
Transformational_Leadership_Style	The management always seeks for changes related to ISPs.	[39]
	The management always seeks for improvements related to ISPs.	
	The management always encourages me to comply with ISPs.	
	The management always educates me on the importance of practicing information security behaviour.	
	The management always reminds me to practice recommended information security behaviour.	
Transactional_Leadership_Style	The management provides incentives to their employees who comply with ISPs.	
	The management always checks to ensure I comply with ISPs	
	The management takes serious action on those who do not comply with ISPs.	
	The management strictly documents the ISPs that everyone should follow.	
	The management is aware of their employees' weaknesses when it comes to their understanding towards information security.	
	The management believes that my job performance will increase if I adopt recommended information security behaviour.	
ISPs_Training_Support	The management always provides specific training on information security.	[42]
	The management encourages me to attend the information security trainings	
	The management organizes information security training effectively.	
	The management updates me on the changes related to ISPs.	
	ISPs training in my organization help me to understand how to behave appropriately towards matters related to information security.	
PU_Security	I believe that information security can reduce security incidents in my organizations.	Self-definition
	I believe that information security can protect my organization's data.	
	I believe that information security can avoid unauthorised access.	
PU_Security-Countermeasure	I believe that changing passwords regularly is effective for avoiding unauthorised access.	Self-definition
	I believe that using anti-virus regularly can protect my computer.	
	I believe that updating anti-virus regularly can protect my computer.	
	I believe that scanning files and devices before using them can protect my computer.	
PEOU_ISPs	I find it easy to understand the ISPs in my organization.	[10]
	I find it easy to comply with the ISPs in my organization.	
	I feel confident with the ISPs in my organization.	
User's information security compliance Behaviour	I comply with ISPs when performing my daily work.	[31]
	I tend to comply with ISPs only when it is convenient to do so.	
	I practice recommended information security behaviour as much as possible.	

Table 2: Measurement Items.

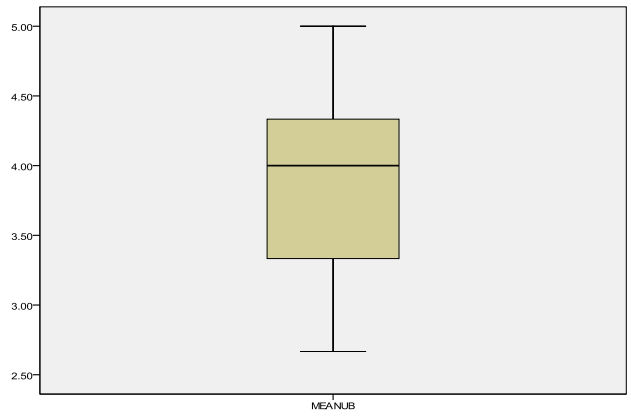

Figure 2: Outliers detection
MEANUB: Mean for user's information security compliance behaviour.

Respondents

The respondents in this study were employees working as health professionals and Information Technology (IT) officers in the Serdang Hospital. A total of 50 questionnaires were distributed randomly. However, only 42 questionnaires were obtained and validated. Another eight questionnaires were rejected due to missing values.

Tests	Results
Keiser-Meyer-Olkin (KMO) measure of sampling adequacy	0.564
Bartlett's test of sphericity	
Approximation Chi-square	857.057
Degree of freedom	276
Significance	.000

Table 3: KMO and Bartlett's test.

The descriptive result indicated that there were more female respondents (90.5%) than male (9.5%). Majority of the respondents were aged between 20-40 years (71.5%). Meanwhile, the respondents with age above 40 years were 28.5%. The result reported that 61.9% of the respondents have more than 10 years of working experiences in the hospital compared to respondents working less than 10 years (38.1%). Most of these respondents were nurses (76.2%), followed by doctors (14.3%), pharmacist (2.4%), and IT officers (7.1%).

Data analysis

In the preliminary study, we used Statistical Package for Social Science (SPSS) 18 to analyse the data. Before analysis, the data was screened for univariate outliers. The result shows that there were no outliers as shown in figure 2. As this is only a preliminary study, the sample size of 42 was deemed to be sufficient. Additionally, exploratory factor analysis is appropriate for small sample size (<50) if the communalities values are high with the range 0.8 to 0.9 [50].

Factor	Item Text	Factor Loading	Eigenvalues	% of Variance
(1) ISPs_Training_ Support (α=.905)	The management encourage me to attend the information security training that is being organized.	.920	7.101	29.589
	The management believe my job performance will increase if I adopt recommended information security behaviour.	.909		
	ISPs training in my organization help me to understand how to behave appropriately towards matter related to information security.	.845		
	The management is aware of their employees' weaknesses when it comes to their understanding towards information security.	.710		
	The management always provides specific training on information security.	.707		
	The management organizes information security training effectively.	.664		
	The management provide incentives to their employees who comply with ISPs.	.642		
(2) PU_Security (α=.870)	I believe that information security can reduce security incidents in my organizations.	.896	5.627	23.447
	I believe that information security can protect my organization's data.	.850		
	I believe that information security can avoid unauthorised access.	.804		
(3) PEOU_ ISPs (α=.917)	I find it easy to understand the ISPs in my organization.	.948	1.937	8.070
	I find it easy to comply with the ISP in my organization.	.919		
	I feel confident with ISP in my organization.	.851		
(4) Transactional_ Leadership_ Style(α=.865)	The management updates me on the changes related to ISPs.	.815	1.722	7.175
	The management take serious action on those who do not comply with ISPs.	.810		
	The management always checks to ensure me comply with ISPs	.742		
	The management strictly documents the ISPs that everyone should follow.	.584		
(5) PU_Security-Countermeasure (α=.825)	I believe that changing password regularly is effective for avoiding unauthorised access.	.853	1.480	6.166
	I believe that using anti-virus regularly can protect my computer.	.668		
	I believe that update anti-virus regularly can protect my computer.	.556		
	I believe that scanning files and devices before use it can protect my computer.	.552		
(6) Transformational_ Leadership_Style (α=.800)	The management always remind me to practice recommended information security behaviour.	.934	1.061	4.419
	The management always educates me on the importance of practicing information security behaviour.	.684		
	The management always seeks for improvements related to ISPs.	.505		
	Cumulative % of Variance Values:			**78.87%**

Table 4: Factor loadings based on a principle components analysis with Promax (N=42).

Factor	Mean	SD
PU_Security	4.18	0.43
PU_Security-Countermeasure	3.99	0.46
Transformational_Leadership_Style	3.85	0.59
PEOU_ISPs	3.79	0.52
Transactional_Leadership_Style	3.46	0.66
ISPs_Training_Support	3.29	0.67
Overall average:	**3.76**	**0.56**

Table 5: Descriptive analysis for users' perceptions on compliance behaviour towards information security.

Results

Exploratory factor analysis

The first exploratory factor analysis was conducted with the 26 items used to measure the independent variables. As the sample size is only 42, a preliminary test involving Kaiser-Mayer-Olkin (KMO) and Bartlett's tests were carried out (Table 3). The KMO overall measure of sampling adequacy was 0.564 and the Bartlett's test of sphericity was 857.057, suggesting that the data can be appropriately used for factor analysis (Table 3).

Using principle component analysis with Promax rotation, the factor analysis yielded a 6-factors solution, which explained approximately 79% of the total variance (eigenvalues greater than 1). A total of 24 items were included. Table 4 illustrates the final rotated factor as well as the statistical data relating to each factor and indicator. The reliability analysis was assessed using Cronbach's Alpha and the values are also presented in table 4.

Referring to table 4, the first factor contained four items measuring information security policies training and three items measuring transactional leadership style. As most of the items relate to the training and support provided, this factor was named ISP_Training_Support. This factor explained almost 30% of the total variance. Meanwhile, the second factor explained 23% of the total variance and contained three items measuring perceived usefulness of security, therefore this factor was named PU_Security. Three items measuring perceived ease of use of information security policies loaded into factor three, therefore this was named PEOU_ISPs with 8% of the total variance. The fourth factor contained three items measuring transactional leadership style and one item measuring information security policies training. As majority of the items measured the leadership style, this factor was named Transactional_Leadership_Style. This factor explained 7% of the total variance. Factor five explained 6% of the total variance and contained four items measuring perceived usefulness of security-countermeasure; therefore this factor was named PU_Security-Countermeasure. Finally, factor six contained three items measuring transformational leadership style, therefore this factor was named Transformational_Leadership_ Style, in line with the definition provided by Burns [10]. This factor explained 4% of the total variance. However, two items used to measure transformational leadership style were excluded due to a low factor loading (<0.5). They were

(i) "The management always seeks for changes related to ISPs" and

"The management always encourages me to comply with information security policies".

(ii) The results also showed that the Cronbach's Alpha values for all six factors exceeded 0.80, well above the minimum value of 0.70 that is considered acceptable.

User's compliance behaviour analysis

Additionally, a descriptive analysis was carried out to analyse users' overall perceptions on their compliance behaviour related to information security. Table 5 shows the results of this analysis, with the factors sorted according to their mean values (ascending order).

Overall, all the mean values for the factors were high (more than 3.0) indicating that majority of the respondents believe these factors affect their compliance behaviour towards information security. PU_Security scored the highest mean (4.18) indicating the majority of the respondents felt that perceived usefulness of security to be the most important factor. This is closely followed by PU_Security-Countermeasure (3.99). All the factors scored more than the overall average value (i.e. 3.76), except for Transactional Leadership Style and ISPs Training. Comparatively, it can be concluded that majority of the respondents in this study emphasized more on factors related to security technology than management support.

Discussion

One of the major issues in information security threat is human error due to their careless behaviour, ignorance or unwillingness to comply with organization's ISPs. This problem can be minimised by having and practising the right user behaviour. Therefore, this study was undertaken to identify the possible factors that can influence user's information security behaviour.

Exploratory factor analysis revealed six factors that affect user's behaviour towards information security: ISP_Training_Support, PU_Security, PEOU_ISPs Transactional _Leadership_Style, PU_Security-Countermeasure and Transformational_Leadership_Style. Similar with previous studies, ISPs training and superior behaviour were found to be important factors that can influence user's compliance behaviour towards information security [9,41,51]. Leadership styles were studied extensively in project management studies as it is one of the important elements in management [52]. Leaders are able to lead their followers in the organization through disciplines and motivate them to give full commitment in terms of practicing information security behaviour [53]. This is supported by other previous studies which revealed top management support can influence employees to comply and practice information security behaviour by providing clear information security guidelines, and strictly monitor and control their employees' behaviour [27,54].

Besides showing positive information security behaviour, top management must be able to implement the effective information security training that can deliver the ISPs message to their employees successfully [27]. Effective information security training is able to increase employees' understanding and awareness. The training program should be implemented regularly as human always forget on what they have been told and learnt. Therefore, top management must play a role in designing information security training programs that are able to create awareness of the importance of complying with organization's ISPs and practicing it adequately [55]. The emergence of Transformational_Leadership_Style, Transactional_Leadership_Style and ISP_Training_Support indicate that majority of the respondents in this study emphasized on the importance of management support.

As for security technology three factors were yielded: PU_Security, PU_Security-Countermeasure, and PEOU_ ISPs. Similar with previous studies, if users' perception towards the information security and security-countermeasure is high, they will tend to comply with the information security policies and regulations [56]. This is supported by a previous study that found PEOU and PU influenced employees to comply with ISPs [32]. This study believes that if users perceive usefulness of security, they will perform adequate behaviour and try to avoid any deviant behaviour that can harm their reputation as an employee in the organization.

Besides users' perception toward the importance of information security, their perception of security-countermeasure must be positive, as indicated by the second factor, PU_Security-Countermeasure. If security-countermeasure is complicated, for example creating strong password and changing the password regularly, users may not behave accordingly [57]. Security-countermeasure should be useable, not complicated and security software installed must have user-friendly interface.

Finally, organizations should consider user's perspective when developing ISPs. The ISPs must be simple, clear and easy to understand, so that users are more likely to practice information security behaviour properly. One of the reasons of information security breaches is the vagueness of ISPs documentation [58]. Therefore, it must be well designed and well enforced by top management and it should be standardised.

Descriptive analysis has revealed that majority of the respondents believe the indicator factors affect their compliance behaviour towards information security and emphasized more on factors related to security technology than management support. The most important factor was PU_Security indicating the majority of the respondents felt that perceived usefulness of security to be. This is supported by previous literatures that if users perception toward security is high, than they are more likely to comply with organization's ISPs and practice security behaviour adequately [59,60].

Conclusion

Human error is one of the major issues should be discussed as it could be the greater risk to health institutions if not managed and controlled accordingly and frequently [61]. This study was reviewed several theory and models to develop research framework with the aims to identify possible factors affecting user's compliance behaviour towards information security. Exploratory factor analysis was conducted to identify possible factors using principal component analysis with promax rotation. The results revealed that transformational leadership style, transactional leadership style, ISPs training, perceived usefulness of security, perceived usefulness of security-countermeasure, and perceived ease of use of ISPs are the factors that can affect user's compliance behaviour towards information security in the context of the management support and security technology. Descriptive analysis result indicated that majority of the respondents agreed the indicated factors can influence users to comply with ISPs. However, the instruments items need to be revised and improved in order to get finest result and more factors should be identified and investigated that can be used in the future research, to study factors influencing users' behaviour towards the information security.

Result of analysis will lead researcher to improve the measurement items that can be used for future investigation. This study has revealed that some of the items have no or little distinction and some even

confused the respondents. The statement then should be well-written and validated. Therefore, comprehensive studies and surveys based on the well-established factors that affect the user's information security compliance behaviour of which this study had attempted to concentrate on, is much needed in the future. Health professionals might have different characteristics towards complying with information security policies, thus it is important for researcher to dig out more on the issues for final study.

Acknowledgement

Our thanks and appreciation goes to all of the respondents who participated in this study. We would also like to thank the Ministry of Health for the permission granted to conduct the survey at the hospitals.

References

1. Hu D, Xu W, Shen H, Li M (2005) Study on information system of health care services management in hospital. Services Systems and Services Management, Proceedings of ICSSSM '05. 2005 International Conference.
2. Rhee H-S, Kim C, Ryu YU (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security 28: 816-826.
3. Kreicberge L (2010) Internal threat to information security-countermeasures and human factor with SME, in Business Aministration and Social Sciences. Lulea University of Technology 1-66.
4. Leach J (2003) Improving user security behaviour. Computers & Security 22: 685-692.
5. Siponen M, Pahnila S, Mahmood MA (2010) Compliance with Information Security Policies: An Empirical Investigation. Computer 43: 64-71.
6. Boujettif M, Wang Y (2010) Constructivist Approach to Information Security Awareness in the Middle East. Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference.
7. Samy NG, Ahmad R, Ismail Z (2010) Security threats categories in healthcare information systems. Health Informatics J 16: 201-209.
8. Huang E, Chuang MH (2007) Extending the theory of planned behavior as a model to explain post-merger employee behavior of IS use. Comput Human Behav 23: 240-257.
9. Bass BM (1985) Leadership and performance beyond expectation.The Free Press, New York.
10. Burns JM (1978) Leadership, Harper and Row , New York.
11. Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of Information Technology. MIS Quaterly 13: 319-340.
12. Ifinedo P (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31: 83-95.
13. Chenoweth T, Minch R, Gattiker T (2009) Application of Protection Motivation Theory to Adoption of Protective Technologies. 42nd Hawaii International Conference.
14. Egea JMO, Gonzalez MVR (2011) Explaining physicians' acceptance of EHCR systems: an extension of TAM with trust and risk factors. Comput Human Behav 27: 319-332.
15. Kim C, Wang T, Namchul S, Kim K-S (2010) An empirical study of customers' perceptions of security and trust in e-payment systems. Electron Commer Res Appl 9: 84-95.
16. Siwei D, Xiaoping Y (2009) An Improved Motivation Model for People Behaviors Change in Virtual Communities Based on Social Cognitive Theory. Information Science and Engineering (ICISE) 1st International Conference.
17. Moller S, Ben-Asher N, Engelbretch K-P, Englert R, Meyer J (2011) Modeling the behavior of users who are confronted with security mechanisms. Computer & Security 30: 242-256.
18. Cox DN, Koster A, Russell CG (2004) Predicting intentions to consume functional foods and supplements to offset memory loss using an adaptation of protection motivation theory. Appetite 43: 55-64.
19. Fry M-L, Dann S (2002) Message processing: Targetting high at-risk group. Proceedings of the Australian & New Zealand Marketing Conference, Melbourne.
20. Lwin MO, Li B, Ang RP (2012) Stop bugging me: An examination of adolescents' protection behavior against online harassment. J Adolesc 35: 31-41.
21. Bonar EE, Rosenberg H (2011) Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies. Addict Behav 36: 1038-1044.
22. Bylund CL, Galvin KM, Dunet DO, Michele R (2011) Using the Extended Health Belief Model to understand siblings' perceptions of risk for hereditary hemochromatosis. Patient Educ Couns 82: 36-41.
23. Buglar ME, White KM, Robinson NG (2010) The role of self-efficacy in dental patients' brushing and flossing: Testing an extended Health Belief Model. Patient Educ Couns 78: 269-272.
24. Gammage, Kimberley L, Klentrou, Panagiota (2011) Predicting osteoprosis prevention behaviors: Health Belief and Knowledge. Am J Health Behav 35: 371-382.
25. Liang H, Xue Y (2009) Avoidance of information technology threats: a theoretical perspective. MIS Quaterly 33: 71-90.
26. Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. Computers & Security 24: 472-484.
27. Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis Support Sys 47: 154-165.
28. Seppo P, Mikko S, Adam M (2007) Employees' Behavior towards IS Security Policy Compliance. 40th Annual Hawaii International Conference.
29. Da Veiga A, Eloff JHP (2010) A framework and assessment instrument for information security culture. Computers & Security 29: 196-207.
30. Huang D-L, Rau PP-L, Salvendy G, Gao F, Jia Z (2011) Factors affecting perception of information security and their impacts on IT adoption and security practices. Int J Hum Comput Stud 69: 870-883.
31. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation. 43rd Hawaii International Conference.
32. Al-Omari A, El-Gayar O, Deokar A (2012) Security Policy Compliance: User Acceptance Perspective. 45th Hawaii International Conference.
33. Bulgurcu B, Cavusoglu H, Benbasat I (2009) Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors. CSE '09 International Conference.
34. Eminağaoğlu M, Uçar E, Eren S (2009) The positive outcomes of information security awareness training in companies–A case study. Information Security Technical Report 14: 223-229.
35. Ng B-Y, Kankanhalli A, Xu Y (2009) Studying users' computer security behavior: A health belief perspective. Decis Support Sys 46: 815-825.
36. Yap CS, Soh CPP, Raman KS (1992) Information system success factors in small business. Omega 20: 597-609.
37. Brady JW (2011) Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. 44th Hawaii International Conference.
38. Aarons GA (2006) Transformational and transactional leadership: Association with attitudes toward evidence-based practice. Psychiatr Serv 57: 1162-1169.
39. Kaushal, S (2011) Effect of leadership and organizational culture on information technology effectiveness: A review. Research and Innovation in Information Systems (ICRIIS) International Conference.
40. Lo M-C, Ramayah T, de Run EC (2010) Does transformational leadership style foster commitment to change? The case of higher education in Malaysia. Procedia Soc Behav Sci 2: 5384-5388.
41. Koskosas I, Kakoulidis K, Siomos C (2011) Examining the linkage between information security and end-user trust. International Journal of Computer Science & Information Security 9: 21-31.
42. Martin N, Rice J (2011) Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security 30: 803-814.

43. Maru K, Fujii Y, Sugita Y, Ohta N, Yoshiura N, et al. (2010) Security of communities based on the e-JIKEI Network with IT and altruism. Procedia Soc Behav Sci 2: 88-94.

44. Kim DJ, Ferrin DL, Rao HR (2008) A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decis Support Sys 44: 544-564.

45. Shen D, Laffey J, Lin Y, Huang X (2006) Social influences for perceived usefulness and ease-of-use of course delivery system. Journal of Interactive Online Learning 5: 270-282.

46. Doherty NF, Anastasakis L, Fulford H (2011) Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. Int J Inf Manage 31: 201-209.

47. Vu K-PL, Proctor RW, Bhargav-Spantzel A, Tai B-L, Josua C, et al. (2007) Improving password security and memorability to protect personal and organizational information. Int J Hum Comput Stud 65: 744-757.

48. Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. Comput Human Behav 24: 2799-2816.

49. Hagen JM, Albrechtsen E, Hovden J (2008) Implementation and effectiveness of organizational information security measures. Information Management & Computer Security 16: 377-397.

50. de Winter JCF, Dodou D, Wieringa PA (2009) Exploratory factor Analysis With Small Sample Sizes. Multivariate Behav Res 44: 147-181.

51. Straub DW (1990) Effective IS security: An empirical study. Information Systems Research 1: 255-276.

52. Hui W, Tsui AS, Xin KR (2011) CEO leadership behaviors, organizational performance, and employees' attitudes. The Leadersh Q 22: 92-105.

53. Michaelis B, Stegmaier R, Sonntag K (2010) Shedding light on followers' innovation implementation behavior. Journal of Managerial Psychology 25: 408-429.

54. Al-Salihy W, Ann J, Sures R (2003) Effectiveness of information systems security in IT organizations in Malaysia. The 9th Asia-Pacific Conference on Communications 2: 716-720.

55. Jenkins JL, Durcikova A, Burns MB (2012) Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior. 45th Hawaii International Conference.

56. Yeh Q-J, Chang AJ-T (2007) Threats and countermeasures for information system security: A cross-industry study. Information & Management 44: 480-491.

57. Renaud K (2012) Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches? Security & Privacy, IEEE 10: 57-63.

58. Luethi M, Knolmayer GF (2009) Security in Health Information Systems: An Exploratory Comparison of U.S. and Swiss Hospitals. HICSS '09, 42nd Hawaii International Conference.

59. Gunson N , Marshall D, Morton H, Jack M (2011) User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security 30: 208-220.

60. Yenisey MM, Ozok AA, Salvendy G (2005) Perceived security determinants in e-commerce among Turkish university students. Behaviour and Information Technology 24: 259-274.

61. Ahlan, Rahman A, Arshad, Yusri, Lubis et al. (2011) Implication of human attitude factors toward information security: Awareness in Malaysia Public University. International Conference on Innovation and Management, Malaysia.