Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness

Norshima Humaidi and Vimala Balakrishnan

***Abstract*—Leadership styles play an important role to enhance employee's information security awareness and may lead to proper information security compliance behavior. Therefore, the current study aims to investigate the indirect effect of leadership styles on user's information security policies compliance behavior through the extent of information security awareness. Questionnaires survey were done among health professionals at government hospitals in Malaysia (*N* = 454). Statistical results confirm that transactional leadership style has a direct effect to all information security awareness factors, but the mediation effect on the relationship between transactional leadership and user's information security policies compliance behavior through two intervening variables (severity awareness and benefit of security-countermeasure). Meanwhile, transformational leadership style has a direct effect on benefit of security-countermeasure and no mediation effect with the extent of all the intervening variables. The research findings found that severity awareness and benefit of security-countermeasure awareness were significant predictors of information security policies compliance behavior while susceptibility awareness and perceived barrier were insignificant. Our findings were proven to be beneficial to fellow researchers and management of the organization, especially related to the medical sectors in improving current standards of information security awareness in hospitals.**

***Index Terms*—Transformational leadership, transactional leadership, information security awareness, health belief model, information security policies compliance behavior.**

I. Introduction

Information security is required to protect organization data from information security threat such as virus and unauthorized users. Information security threats can be categorized into two categories: internal threat and external threat. External threat is caused by outsiders and it is not a major issue in information security because many organizations have implemented advanced security technologies such as smart card and biometrics [1], [2]. Until recently, the main critical information security issue identified is internal threat, where is caused by internal factors, mainly the employees' poor users' behavior such as carelessness, user errors and omission [2].

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 [1], [3]. This notion is supported by Boujettif and Yongge [4] 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 Health Information System (HIS) [5]. Human error caused information security incidents because of employees in the organization have lack of recognition of potential threat vulnerabilities, undeveloped understanding of information security and lack of knowledge about information security [6]. Thus, leader plays an important role to encourage and monitor employees in the organization aware on organization information security policies (ISPs) and comply it properly. If employees' awareness of information security is increasing, security incidents in the organization can be reduced. To the best of our knowledge, lack of studies was focus on indirect effect of leadership styles on employees' information security policies compliance behavior. Hence, the current study aims to investigate the indirect effect of leadership styles on user's information security policies compliance behavior through the intervening variable of information security awareness.

The rest of the paper is presented as follows: the next section reviewed information security policies compliance behavior. The third section presents the research framework and discusses the integration theories that were adapted to develop propose research model 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.

II. Information Security Policies Compliance Behavior

ISPs can be implemented more effective, if employees' behavior towards information security can be control and manage accordingly. If this cannot be controlled or monitored carefully, it can pose security threats to organization. The effectiveness of information system's security can be achieved through promoting adequate information security behavior and constraining unacceptable information behavior among employees in the organization [7]. The study believes that if employees' compliance behavior towards information security policies is acceptable, security incidents can be decreased, and effectiveness of

Manuscript received February 27, 2014; revised April 27, 2014. This work was supported under Grant Ministry of Education (MOE), Malaysia.

Norshima Humaidi is with the Faculty of Business Management, University of Technology Mara, Shah Alam, Malaysia and also with the Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia (e-mail: norshima24@yahoo.com).

Vimala Balakrishnan is with the Department of Information System, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia (e-mail: vimala.balakrishnan@um.edu.my).

DOI: 10.7763/IJIET.2015.V5.522

information system's security can be increased. This is supported by other literature stated that security compliance behavior able to promote security assurance behavior [8].Security compliance behavior describes as behavior which do not violate organization ISPs and security assurance behavior is describes as behavior that actively carry out to protect organization IS such as taking security pre-cautions and reporting any security incidents exist in the organization [8].

There are several reasons why users did not comply on security rules and procedures which are they feel the security rules and policy is too strict, lower usability, nuisance, complicated and difficult to follow [9]. In addition, the non-compliance behavior due to user's dissatisfaction due to lower usability of system's security and organization has missing to establish such as optimum trade-off already in the system design phase [10]. There are some factors that lead to non-compliance behavior event though users have given well information security trained but still make mistakes; these are cause by environment, social and organizational factor. If their work environment is stressful, this might reduce their attention and cause error. Social and organizational factors can influence them to comply and behave properly towards information security. If leader did not bother and care to follow the security rules and procedures, so do them. Therefore, it is very important that leader in the organization build up a positive security environment at their work place because it can help to increase information security compliance behavior, hence security incidents can be decreased.

III. Research Model and Hypotheses

The research model was developed by combining leadership style theory and Health Belief Model (HBM) as shown in Fig. 1. This model consists of two leadership styles (transformational leadership and transactional leadership) and perceived barrier as exogenous constructs. Information security awareness as a mediator consists of three constructs (severity awareness, susceptibility awareness and benefit of security-countermeasure awareness). Meanwhile, endogenous construct in the current study is compliance behavior of HIS security policies.

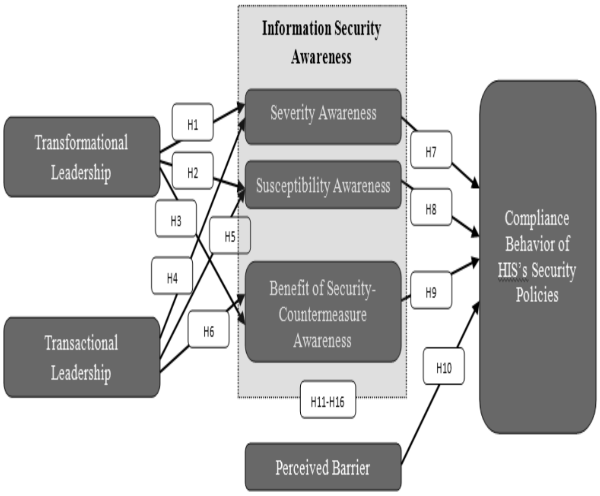

Information Security Awareness
Severity Awareness
Susceptibility Awareness
Benefit of Security-Countermeasure Awareness
Transformational Leadership
Transactional Leadership
Perceived Barrier
Compliance Behavior of HIS's Security Policies
H1
H2
H3
H4
H5
H6
H7
H8
H9
H10
H11-H16

Fig. 1. Proposed research model.

A. Leadership Style

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 [11]. This study focuses on two styles of leadership: transformational leader and transactional leader. Leaders who are engaged with their team members and motivate them is said to have the characteristics of a *transformational leader* [11], 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 [12].

Many leadership studies have shown that both leadership styles have significant influence on employees' work performance [13]. We believe that strong leadership is required in guiding users to make the right decisions and to promote information security awareness among users in terms of threat severity and susceptibility, and benefits of using security-countermeasure to reduce security threats. Therefore, we formulated six research hypotheses as follows:

- H1: Transformational leadership influences severity awareness.
- H2: Transformational leadership influences susceptibility awareness.
- H3: Transformational leadership influences benefit of security-countermeasure awareness.
- H4: Transactional leadership influences severity awareness.
- H5: Transactional leadership influences susceptibility awareness.
- H6: Transactional leadership influences benefit of security-countermeasure awareness.

B. Health Belief Model

Health Belief Model (HBM) is one of the behavioral theory that was developed in the 1950s to explain and predict preventative health behaviors [14]. It has been most widely used in health behavior studies such as drug [15], cancer [16], and dental [17], among others. HBM predicts that if people believe in specific illnesses and know how to prevent the illnesses, they will be more cautious, and therefore practice recommended health behavior [18]. HBM suggests that individuals determine the feasibility, benefits and cost related to an intervention or behavior change based on the following factors: perceived susceptibility (similar to perceived vulnerability), perceived severity, perceived benefit and perceive barrier.

We believe that employees' security behavior can be controlled based on their perception of security threat and how this can help them to perform adequate secure behavior to reduce threat. Perception of security threat is likely to be affected by susceptibility and severity and evaluation of secure behavior is likely to be affected by benefits and barriers and thus, if threat is perceived and secure behavior is chosen, then the users knows how to behave and conduct it properly [19].

HBM has being suggested by previous study to be a comprehensive theory because it consists of number of explanatory constructs that are not represented in IS adoption or other related theories, but important in information security practices [20]. Moreover, HBM is able to measure or predict human behavior successfully [21]. Based on that, the current study suggested that awareness of threat severity; susceptibility and benefit of security-countermeasure are the indicators of information security awareness factor.

C. Information Security Awareness

Severity awareness refers to users' understanding towards the seriousness of information security threats. Meanwhile, susceptibility awareness refers to users' perception towards probability of organization information of being exposed to information security threats. On the other hand, benefit of security-countermeasure awareness refers to the degree to user perceives the positive outcomes of performing certain secure behavior such as using security-countermeasure adequately [16]. We believe that if employees are aware of severity and susceptibility of information security threats, and aware of the benefits of security-countermeasure which can help to protect organization's data and promotes their works, they will likely to avoid any improper security behavior. Thus, the following three research hypotheses were addressed.

- H7: Severity awareness influences users' information security policies compliance behavior.
- H8: Susceptibility awareness influences users' information security policies compliance behavior.
- H9: Benefit of security-countermeasure influences users' information security policies compliance behavior.

D. Perceived Barrier

Ng *et al.* [20] defined perceived barrier as a user's perceptions towards the difficulty of practicing computer security behavior, which is likely to reduce the performance of information security behavior. One of the barriers in information security is unskilled employees towards security technology due to their lack of security awareness. The barriers in information security was the reason why employees did not practice computer security in their workplaces [20]. Therefore, research hypothesis was formulated as follows:

- H10: Perceived barrier influences users' information security policies compliance behavior.

E. Mediation Effect of Information Security Awareness

Management plays an important role to encourage positive users' behavior towards the use of information system [22]. This can be done through style of leadership. Additionally, 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 leaders of the organization can provide a set of clear security guidelines and strictly monitor their employees, information security compliances will also increase [10]. 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 [23]. Therefore, it is essential that the leaders play their role firmly to ensure the effectiveness of information system's security by encouraging and motivating their employees to comply with ISPs and strictly monitor employees' behavior related with information security. The current study believes that the mediating effect of employees' information security awareness will show the relationships between leadership styles and information security compliance behavior. In this regard, we propose the following hypotheses:

- H1: The effect of transformational leadership on users' information security policies compliance behavior is mediated by: (H11) severity awareness; (H12) susceptibility awareness; (H13) benefit of security-countermeasure awareness.
- H2: The effect of transactional leadership on users' information security policies compliance behavior is mediated by: (H14) severity awareness; (H15) susceptibility awareness; (H16) benefit of security-countermeasure awareness.

IV. Research Methodology

The current study was employed quantitative research method, whereby questionnaires were developed based on leadership studies [24] and HBM studies related to information security studies [20], [25], [26].

A. Instrument Development

Questionnaires were prepared in two languages, that is English and Bahasa Melayu (national language). It was divided into three sections: Section A consists of demographic questions such as age, HIS experience, gender and occupation. Section B assesses users' perceptions of leadership styles and security awareness of severity, susceptibility and benefit of security-countermeasure. Finally, Section C focuses on employees' compliance behavior towards HIS security policies. All the indicators in Sections B and C were measured using 5-point Likert-type scale, with anchors ranging from 1 (strongly disagree) to 5 (strongly agree). Altogether, eight measurement items were used to measure exogenous constructs, fourteen items were used to measure mediators and four measurement items were used to measure endogenous construct. The total is 26 measurement items.

B. Data Collection

In the current study, management of three local hospitals in Malaysia agreed to be participants of the study (Serdang Hospital, Selayang Hospital and Sungai Buloh Hospital). The samples of the current study were not homogeneous; thus, stratified random sampling was used to determine sample sizes to ensure that an adequate number of subjects were selected from each category of employees at selected local hospitals. 300 questionnaires were distributed in each local hospital. The respondents in this study were employees working as health professionals (doctors, support staff and health administrators) who are end-users of HIS. A total of 900 questionnaires were distributed randomly to the respondents. However, only 454 questionnaires were returned and validated. Another 421 questionnaires were classified as non-response and 25 questionnaires were rejected due to serious missing values.

C. Respondents

The descriptive results show that there were more females with a total of 357 respondents (78.6%) than males with a total of 97 respondents (21.4%). The majority of the respondents were aged between 20–40 years (*n* = 394, 86.7%), and the rest were more than 40 years old (*n* = 60, 13.2%). Eighty percent of the respondents (*n* = 362) had less than 10 years of HIS working experience in the hospital while the remaining 20% of the respondents (*n* = 92) had been working for more than 10 years. Most of the respondents were support staff (nurses, pharmacists, radiologist, medical assistant, etc.) with a total of 281 respondents (61.9%), followed by doctors (*n* = 129, 28.4%), and health administrators (*n* = 44, 9.7%). The majority of the respondents were from Sungai Buloh Hospital (*n* = 166, 36.6%), followed by Selayang Hospital (*n* = 159, 35%), and Serdang Hospital (*n* = 129, 28.4%).

V. Data Analysis

Statistical Package for Social Science (SPSS) 21.0 was employed to screen data in terms of coding, outliers, normality and assessment of common method bias (CMB). Based on the SPSS results, research data were considered normal. Thus, the SEM-PLS was 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 was used to test the measurement and structural model of the current study. Bootstrapping with 500 re-samples was performed to obtain the statistical significance of path coefficients using a t-test.

TABLE I: Summary of Factor Analysis for Common Method Bias Test

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	10.485	41.941	41.941	10.485	41.941	41.941
2	2.515	10.059	52.001			
3	1.833	7.332	59.333			
4	1.462	5.847	65.180			
5	1.043	4.173	69.352			
6	.734	2.937	72.289			
7	.709	2.838	75.127			
8	.694	2.776	77.903			
9	.589	2.354	80.257			

A. Common Method Bias

Common method bias which is defined as “variance that is attributable to the measurement method rather than to the constructs the measure represent” [27] could be problematic. We used Harman’s single-factor test to assess the CMB. 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 un-rotated single factor analysis was explaining less than 50% percent of the variance as shown in Table I. Given that a single factor solution did not emerge and a general factor did not account for most of the variance, CMV was not viewed as a significance threat in this current study [28]. Thus, all the constructs in the research were tested for confirmatory factor analysis (CFA).

B. Convergence and Reliability Validity

Confirmatory factor analysis was conducted to test how well the developed instrument measures particular constructs in the research model; this was done by examining construct and reliability validity. *Firstly*, as suggested by Hair *et al.* [29], we examined the factor loadings, composite reliability and average variance extracted (AVE) to assess the convergence validity as shown in Table II. The factor loadings for all the indicators exceeded the recommended value of 0.5, which is acceptable [30]. The composite reliabilities (CR) for each construct ranged from 0.874 to 0.923, which exceeded the recommended value of 0.7 [29]. Meanwhile, the AVE for each construct ranged between 0.632 until 0.795, which is greater than 0.5; thus, the cut-off values ensure that at least 50% or more of the variances in the construct are explained by the set of indicators. The collected data have been verified for its reliability by calculating the Cronbach’s Alpha (CA). The resulting value ranged from 0.783 to 0.904, which is acceptable. The results of the measurement model show that all the six constructs are valid measures based on their parameter estimates and statistical significance [29].

Then, we proceeded to test the discriminant validity by examining the squared correlations between the measures of potentially overlapping constructs. The results (Table III) show that all diagonal values in bold were higher than the values in its row and column, indicating adequate discriminant validity; this means no overlapping construct exists.

C. Hypotheses Testing

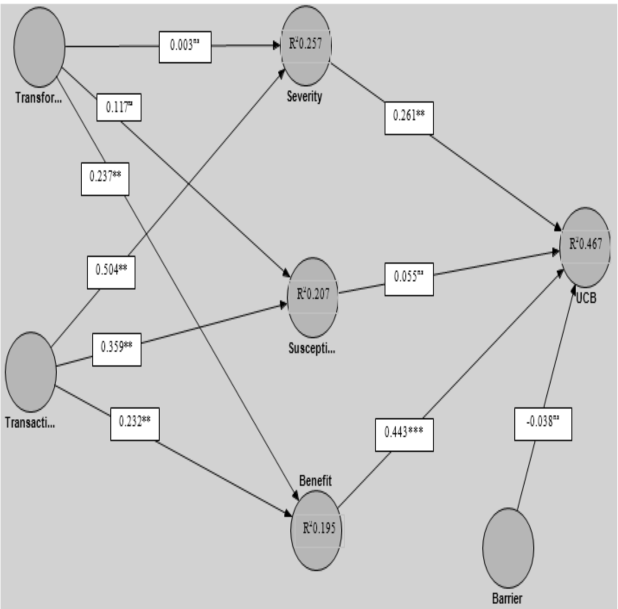
The results show (Fig. 2) that 25.7 percent of variance in severity awareness, 20.7 percent of variance in susceptibility awareness and 19.5 percent of variance in benefit of security-countermeasure awareness were explained by transformational leadership and transactional leadership. Meanwhile, 46.7% of variance in compliance behavior of HIS security policies was explained by severity awareness, susceptibility awareness, benefit of security-countermeasure and perceived barrier.

Transactional leadership was found to have significant influence on severity awareness (β = 0.504, t-value = 6.732**), susceptibility awareness (β = 0.359, t-value = 4.534**) and benefit of security-countermeasure awareness (β = 0.232, t-value = 3.239**). Meanwhile, transformational leadership was found to has significant influence on benefit of security-countermeasure awareness (β = 0.237, t-value = 3.390**) while awareness of severity and susceptibility shown insignificant. Thus, H1 and H2 were not-supported while H3 until H6 were supported.

TABLE II: CONVERGENCE AND RELIABILITY VALIDITY

Constructs	Items	Factor loadings	AVE	CR	R Square	CA
Transformational leadership	Leader always encourages me to comply with ISPs.	0.907	0.795	0.921		0.871
	Leader always seeks for improvements related to ISPs.	0.885				
	Leader always educates me on the importance of practicing ISPs.	0.883				
Transactional leadership	Leader takes serious action against those who do not comply with information security policies.	0.846	0.699	0.874		0.783
	Leader always values the adoption of practising adequate information security behavior.	0.876				
	Leader thinks my job performance will improve if I adopt appropriate information security behavior.	0.784				
Susceptibility	I am aware that if I do not adopt appropriate information security behavior, it will cause security incidents.	0.843	0.703	0.904	0.207	0.858
	I am aware that it is a serious problem if I am not complying with information security policies in my organisation.	0.869				
	I am aware that if I am not complying with information security policies, my organisation could be subjected to serious information security threats.	0.861				
	I am aware that it is a serious problem if organisational data are stolen by unauthorised users.	0.777				
Severity	If I do not follow information security policy, the penalty will be severe.	0.803	0.637	0.875	0.257	0.810
	Failure to adopt information security behavior will worsen information security problem of my organisation.	0.759				
	Failure to adopt information security behavior will jeopardise my career.	0.825				
	Failure to adopt information security behavior will harm my organisation's data.	0.805				
Perceived Barrier	Implementing information security behavior such as scanning files is a waste of time.	0.839	0.809	0.894		0.783
	Adopting information security behavior is inconvenient.	0.956				
Benefit of security-countermeasure	I am aware that using information security countermeasure is effective for reducing the number of security incidents in my organisation.	0.790	0.632	0.923	0.195	0.904
	I am aware that information security countermeasure is effective for protecting my organisation's data.	0.782				
	I am aware that using a strong password is effective for avoiding unauthorised access.	0.828				
	I am aware that changing my password regularly is effective for avoiding unauthorised access.	0.759				
	I am aware that using anti-virus regularly is effective for protecting my computer.	0.811				
	I am aware that updating anti-virus regularly is effective for protecting my computer.	0.835				
	I am aware that scanning files and devices before using them is effective for protecting my computer.	0.755				
HIS security policies compliance behavior	I comply with information security policies when performing my daily work.	0.841	0.726	0.914	0.468	0.875
	I practise recommended information security behavior as much as possible.	0.877				
	I always recommend others to comply with information security policies.	0.840				
	I assist others in complying with information security policies.	0.849				

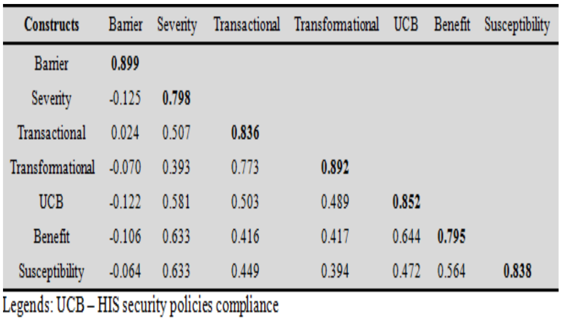
The results also show that severity awareness (β = 0.261, t-value = 4.478**) and benefit of security-countermeasure awareness (β = 0.443, t-value = 8.873***) were found to have significant influence on compliance behavior of security policies related to HIS. Meanwhile, susceptibility awareness was not significant (β = 0.055, t-value = 0.942) and perceived barrier was found negatively insignificant (β = -0.038, t-value = 1.085). Overall, it was found that awareness of benefit of security-countermeasure was the most significant predictor of HIS's security policies compliance behavior. These results provide support for H7 and H9 whereas H8 and H10 are not supported.



Mediation effects: H11^{ns,}, H12^{ns}, H13**, H14**, H15^{ns}, H16**
Significance Level: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$, ns – not significance.

Fig. 2. Results for the research model.

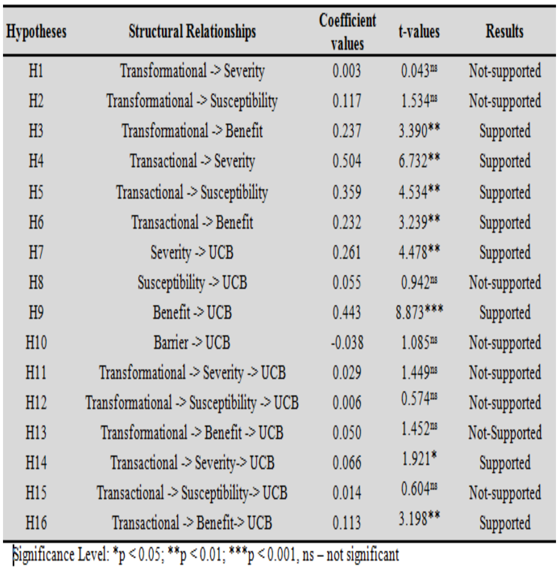
TABLE III: DISCRIMINANT VALIDITY



Constructs	Barrier	Severity	Transactional	Transformational	UCB	Benefit	Susceptibility
Barrier	**0.899**						
Severity	-0.125	**0.798**					
Transactional	0.024	0.507	**0.836**				
Transformational	-0.070	0.393	0.773	**0.892**			
UCB	-0.122	0.581	0.503	0.489	**0.852**		
Benefit	-0.106	0.633	0.416	0.417	0.644	**0.795**	
Susceptibility	-0.064	0.633	0.449	0.394	0.472	0.564	**0.838**

Legends: UCB – HIS security policies compliance

TABLE IV: HYPOTHESES RESULT



Hypotheses	Structural Relationships	Coefficient values	t-values	Results
H1	Transformational -> Severity	0.003	0.043^{ns}	Not-supported
H2	Transformational -> Susceptibility	0.117	1.534^{ns}	Not-supported
H3	Transformational -> Benefit	0.237	3.390**	Supported
H4	Transactional -> Severity	0.504	6.732**	Supported
H5	Transactional -> Susceptibility	0.359	4.534**	Supported
H6	Transactional -> Benefit	0.232	3.239**	Supported
H7	Severity -> UCB	0.261	4.478**	Supported
H8	Susceptibility -> UCB	0.055	0.942^{ns}	Not-supported
H9	Benefit -> UCB	0.443	8.873***	Supported
H10	Barrier -> UCB	-0.038	1.085^{ns}	Not-supported
H11	Transformational -> Severity -> UCB	0.029	1.449^{ns}	Not-supported
H12	Transformational -> Susceptibility -> UCB	0.006	0.574^{ns}	Not-supported
H13	Transformational -> Benefit -> UCB	0.050	1.452^{ns}	Not-Supported
H14	Transactional -> Severity-> UCB	0.066	1.921*	Supported
H15	Transactional -> Susceptibility-> UCB	0.014	0.604^{ns}	Not-supported
H16	Transactional -> Benefit-> UCB	0.113	3.198**	Supported

Significance Level: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$, ns – not significant

The current study found that benefit of security-countermeasure mediated the relationship between transactional leadership and compliance behavior of security policies related to HIS (β = 0.113, t-value = 3.198**). The mediation effect of severity awareness was also significant in the relationship between transactional leadership and compliance behavior of security policies related to HIS (β = 0.066, t-value = 1.921*), but not for transformational leadership. Transformational leadership and transactional leadership have no indirect effect through the extent of susceptibility awareness. Therefore, based on the mediation results, H14 and H16 are supported whereas H11, H12, H13 and H15 are not supported. All the hypotheses testing result are presented in Table IV.

VI. DISCUSSION

A. Discussions of Findings

The results show that transactional leadership style is the most influences employees' awareness on threat severity and susceptibility while transformational leadership style was insignificant. This indicates that employees' information security awareness was enhanced when leader clarified rewards of performance and expressed satisfaction with the achievements of their employees in the organization related with information security policies compliance behavior. Both of leadership styles influences user's awareness of the benefits of using security-countermeasure in their daily task. This is proved that leader should not only encourage but also enforce employees to use security-countermeasure properly to prevent information security threats and practice information security behavior as recommended by the organizations.

Awareness of threat severity and benefit of security-countermeasure were affect information security compliance behavior among employees. This is in line with many previous researchers found that perceived severity and perceived benefit can influence compliance behavior towards organization's ISPs [31]-[33]. On the other hand, susceptibility awareness does not seem to affect employees' compliance behavior towards organization ISPs. This is different than previous findings which found that perceived susceptibility was a determinant of computer security behavior [20] and it is also influences employees to comply with organization ISPs [26]. Health professionals who are the respondents of the current study maybe have different perception of health data susceptible to security risk that lead to non-significant result. However, the results might be changed if more health professionals responses on the survey.

Transactional leadership has significant direct and indirect effect on user's information security policies compliance behavior through severity awareness and benefit of security-countermeasure awareness while transformational leadership has no indirect effect on user's information security policies compliance behavior through all intervening variables. The mediating results show that transactional leadership style more powerful than transformational leadership style when related to information security compliances behavior among health professionals through information security awareness factors. Strong transactional leadership in the form of contingent rewards and strictly punish employees who not comply and practice information security behavior properly may lead to situations which deeper level of information security awareness are formed, thereby increasing information security compliance behavior.

B. Limitations and Future Work

This study collected data from self-reports that may result in common method variance (CMV). However, this issue cannot be avoided because of social desirability and the respondent's consistency motif [28]. The current study has verified that CMV did not influence the data and the data is acceptable. However, future research should enhanced the techniques used in this study to get more finer data and explore more factors that can mediated the relationship between leadership styles and user's information security compliance behavior such as user's information security skills.

VII. Conclusions

In the current study, we developed research model using leadership theory and HBM, and empirically examined how leadership styles works through intervening variables (severity awareness, susceptibility awareness and benefit of security-countermeasure awareness) that influences information security policies compliance behavior among health professionals. The results have implications on managerial aspects, whereby transactional leadership style has direct and indirect effect on user's information security compliance behavior through severity awareness and benefit of security-countermeasure awareness. This is indicated that strict leadership able to increase user's awareness of information security, thus encourage information security compliance behavior.

However, the indicators used to measure each indicated constructs need to be revised and improved in order to get finer result and more constructs should be dug out and investigated that can be used in future research, to study factors influencing users' behavior towards the security policies related with HIS. Health professionals might have different perceptions towards complying with information security policies, thus, it is important for researcher to dig out more on the issues. Other limitation is that, the current study collected data from self-reports, that may result in common method variance (CMV). However, this issue cannot be avoided because of social desirability and the respondent's consistency motif [28]. The current study has verified that CMV did not influence the data and the data is acceptable. However, future research should enhance the research technique used in this study to get more data and explore more factors, to study users' compliance behavior towards the security policies related with HIS.

In conclusion, the current study showed that the research model was valid based on PLS analysis and also contributes in a human compliance behavior study use the aspects of information security awareness. In addition, the research findings will also prove to be beneficial to management of the organization in improving current method of increasing user's information security awareness. Hence, user's compliance behavior towards ISPs can be improved.

Acknowledgment

Our thanks and appreciation goes to all of the respondents who participated in 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 Education (MOE) for the research grants.

References

[1] L. Kreicberge, "Internal threat to information security - countermeasures and human factor with SME," *Business Aministration and Social Sciences*, 2010, University of Technology, pp. 1-66.

[2] L. John, "Improving User Security Behavior," *Computers & Security*, vol. 22, no. 8, pp. 685-692, 2003.

[3] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, vol. 43, no. 2, pp. 64-71, 2010.

[4] M. Boujettif and W. Yongge, "Constructivist approach to information security awareness in the Middle East," presented at *2*010 International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010.

[5] G. Narayana, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems," *Health Information Journal*, vol. 16, no. 3, pp. 201-209, 2010.

[6] P. A. H. Williams, "In a 'trusting' environment, everyone is responsible for information security," *Information Security Technical Report*, vol. 13, no. 4, pp. 207-215, 2008.

[7] S. Woodhouse, "Information security: End user behavior and corporate culture," presented at 7th IEEE International Conference on Computer and Information Technology- CIT 2007, 2007.

[8] K. H. Guo, "Security-related behavior in using information systems in the workplace: A review and synthesis," *Computers & Security*, 2012.

[9] K. Renaud, "Blaming noncompliance is too convenient: What really causes information breaches?" *Security & Privacy*, IEEE, vol. 10, no. 3, pp. 57-63, 2012.

[10] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectivenes*s*m," *Decision Support Systems*, vol. 47, no. 2, pp. 154-165, 2009.

[11] J. M. Burns, *Leadership*, New York: Harper and Row, 1978.

[12] B. M. Bass, *Leadership and Performance beyond Expectation*, New York: The Free Press, 1985.

[13] S. Kaushal, "Effect of leadership and organizational culture on information technology effectiveness: A review," presented at 2011 International Conference on Research and Innovation in Information Systems (ICRIIS), 2011.

[14] 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, no. 1, pp. 29-36, 2010.

[15] 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, no. 11, pp. 1038-1044, 2011.

[16] C. L. Bylund *et al.*, "Using the extended health belief model to understand siblings' perceptions of risk for hereditary hemochromatosis," *Patient Education and Counseling*, 2011, vol. 82, no. 1, pp. 36-41.

[17] M. E. Buglar, K. M. White, and N. G. Robinson, "The Role of Self-Efficacy in Dental Patients' Brushing and Flossing: Testing an Extended Health Belief Model," *Patient Education and Counseling*, vol. 78, no. 2, pp. 269-272, 2010.

[18] K. L. Gammage and P. Klentrou, "Predicting osteoprosis prevention behaviors: Health belief and knowledge," *Health Behavior*, 2011. vol. 35, no. 3, pp. 371-382.

[19] N. Davinson and E. Sillence, "It won't happen to me: Promoting secure behavior among internet users," *Computers in Human Behavior*, vol. 26, pp. 1739-1747, 2010.

[20] B. Y. Ng, K. Atreyi, and X. Yunjie, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, vol. 4, pp. 815-825.

[21] W. Brown, A. Ottney, and S. Nguyen, "Breaking the barrier: the Health Belief Model and patient perceptions regarding contraception," *Contraception*, vol. 83, no. 5, pp. 453-458.

[22] C. S. Yap, C. P. P. Soh, and K. S. Raman, "Information system success factors in small business," *Omega*, vol. 20, no. 5, pp. 597-609, 1992.

[23] J. W. Brady, "Securing health care: Assessing factors that affect hipaa security compliance in academic medical centers," presented at 2011 44th Hawaii International Conference on System Sciences (HICSS), 2011.

[24] G. A. Aaron, "Transformational and transactional leadership: Association with attitudes toward evidence-based practice," *Psychiatric Services*, vol. 57, pp. 1162-1169, 2006.

[25] Ö. Şimşekoğlu and T. Lajunen, "Social psychology of seat belt use: A comparison of theory of planned behavior and health belief model," *Transportation Research Part F: Traffic Psychology and Behavior*, vol. 11, no. 3, pp. 181-191, 2008.

[26] 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, no. 1, pp. 83-95, 2008.

[27] 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.

[28] P. M. Podsakoff and D. W. Organ, "Self-Reports in organizational research: Problems and prospects," *Journal of Management*, vol. 12, no. 4, pp. 531-544, 1986.

[29] J. F. Hair *et al.*, *Multivariate data analysis: A global perspective*, 7th ed., 2010, Upper Saddle River, New Jersey: Pearson Prentice Hall.

[30] A. L. Comrey, *A First Course in Factor Analysis*, 1973, Academic Press: New York, NY.

[31] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors," presented at 2009 International Conference on Computational Science and Engineering CSE '09, 2009.

[32] J. M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security*, vol. 16, no. 4, pp. 377-397, 2008.

[33] 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, no. 2, pp. 99-110, 2012.

Norshima Humaidi is a senior lecturer at the Faculty of Business Management, University Technology MARA (UiTM), Puncak Alam Campus, Malaysia. She obtained her master of science in information technology from UiTM, Malaysia. Currently, she is PhD candidate at Faculty of Computer Science and Information Technology, University of Malaya (UM), Malaysia.

Her research interests include information security, management information systems and project management. Her researches have been presented and publish in proceedings of IEEE ICAMS 2010, IAM 2011, ICCPM 2011, ICMAI 2012, ICETCIT 2013, 6th International Conference on Construction in the 21st Century, Asia Pacific International Conference on Environment-Behavior Studies, Internal Conference on Innovation and Management 2011, International Journal of Innovation, management and technology (IJIMT), Journal of Information Technology Management (JITM), Journal of Health & Medical Informatics (JHMI) and Australian Journal of Basic and Applied Sciences (AJBAS).

Vimala Balakrishnan is a senior lecturer at the Faculty of Computer Science and Information Technology, University of Malaya (UM), Kuala Lumpur, Malaysia.

Her Ph.D. was in the field of ergonomics, particularly related to mobile phone applications and usability studies. Currently most of her research work revolves around data/knowledge engineering in health informatics and information security.