Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility

Abdul Rahman Ahlan
Information Technology Division (ITD)
International Islamic University of Malaysia (IIUM)
Selangor, Malaysia
arahman@iium.edu.my

Muharman Lubis
International Islamic University of Malaysia
Selangor, Malaysia
muharman.lubis@gmail.com

Abstract— **As the 21st century approached, the current trend of technology product besides deliver the benefit on availability and accessibility on information, problem emerged regard information security. In order to analyze on how technology introduces new risks, it is necessary to discuss the technology lifecycle. Consider for instance the life cycle of technology as the diffusion of an innovation. Since technological innovations or IT solutions are being adopted to support business processes, the need to protect those IT solutions arises with its adoption. Accordingly, two important factors need much consideration in raising awareness are how organization influences significantly of end user's attitude and how the organization has the regular assessment or evaluation to measure the effectiveness of IS awareness policy inside the organization.**

Keywords; information security awareness; learnability; adaptability; performance; roles of responsibility

I. INTRODUCTION

A tremendous amount of technology-related innovation and change has occurred over the past decade in relation for the increasing demands on the technology needs in market area. The possible causes might be several and varied, for example, sudden changes of human attitude that are not following the established information security procedures because less attention or less familiar. It could compromise organization integrity leads to bad influence internally and externally. Moreover, the lack of security procedures under determined circumstances and the lack of mechanisms to evaluate the effectiveness of the Information Security Awareness (ISA) Program, they also may lead to undesired results with unexpected consequences. Therefore, while the procedure and mechanism could be measure through several criteria or checklist, it's different on the human attitude. The organization should manage and organize human attitude as the valuable assets accordingly to be benefit to them.

Many universities are still vulnerable from exploitation especially the human attitude threats. In general, ISA concerns on the degree of user understanding towards the importance of information security that will affect the university process on how end user response and act in facing the possible weaknesses emerged. To enhance the ISA towards the user's attitude, the comprehensive study is encouraged in terms of the user's perception and understandings consider that each environment has the unique characteristic compared to the others. Therefore, this paper aims to bridge the gap in literature and practical by examining how human attitude as the factor influence ISA positively for supporting university's policies. In this research, assessment process based on adjustment of current framework and prototype, which will evaluate the concept reliability in the environment. Hence, we argue that research in ISA is limited in that; it does not provide details on how to utilize the human factors to improve ISA consider human threats as greatest risk. The paper review the literature in the area briefly, justifies the methods and variable, discusses the result and limitations and concludes by discussing further research directions in the area.

II. LITERATURE REVIEW

Information security issue already become top priorities in various institutions and strongly related to the concept of risk. According to the Information Security Forum [4], security awareness is defined as "*the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities and act accordingly*". Meanwhile, Siponen [10] defined security awareness as "*a state where users in an organization are aware, ideally committed to, of their security mission*".

Study by Tolnai and von Solms [11] suggested the use of portal to raise the awareness among the community consider that most activities right now such as online transaction, banking and service have done through Internet. He said the missing point in the ISA is comprehensive knowledge in understanding of security, privacy and safety risk to have activities through Internet that might be compromised in the wrong hands. Interestingly, he also suggested the use of graphical interface to catch the end user attention and encourage interactivity that have similar principle like previous study suggest as the solution [2][9][13]. Furthermore, assessing the perception or expectation is important in analyzing the following issues like the way behaving on the works, actual habits which influences motivation towards improvement and user concerns of responsibility.

The significant changes in the organization could not be immediately; the alignment of organization goals,

policies and procedures are really encouraging to deliver message on how serious the issues in Information Security into environment as well as the commitment to protect the end user privacy' which related to job position in the organization. Positive job attitude creates a tendency to engage or contribute desirable inputs to one's work role, rather than withhold them [16]. Therefore, Bulgurcu [1] emphasized the importance of the role of an employee's ISA and her perceived fairness of the requirements of the ISP. Their challenge is novel and has a lot of common features with our purpose in this paper. At last, the attempt to investigate relationships between employee's ISA and some individual or organizational attributions by using data in Japan collected from a Web-based survey [14] found employee's ISA is different in some organizational attributes such as situations on prohibited matter with handling of information in organization. He claims that enhancing information security education is efficient measure, not just introducing new information security tools.

III. METHODOLOGY

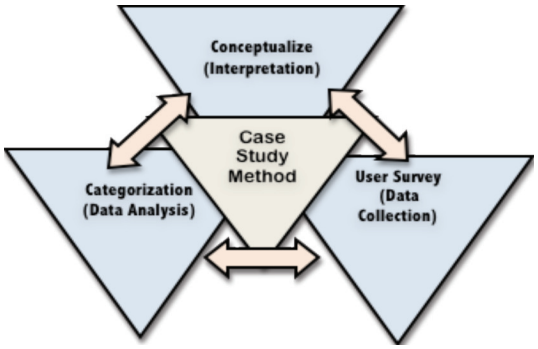

Figure 1. Research Methodology.

A. Participants and Procedure

The population included in this study will be admin staff, academic staff, undergraduate and postgraduate student from International Islamic University of Malaysia (IIUM). The selection process will relate conclusively with the institution in IT or the user that have knowledge in IT as their background. Hence, 306 users involve 207 students (107 undergraduate and 100 postgraduate) and 99 staffs (48 academic and 51 administration) will participate for the survey method and the selected one will be continue for the interview. In addition, all of participants will be under naturalistic for further details and data gathering.

B. Instrument

This study will use quantitative methodology, which was survey questionnaire through online approach as the data collection method. Previously, pre test towards 2 experts and pilot study towards 15 people will be conducted to evaluate the quality of questionnaire form. In the online approach, targeted user will receive link e-mail of survey to fill the answer, which based on automatic key generated from the sender so selected person only can access the questionnaire and answer the question, while the notification will emerge to the sender. The questionnaire will be divided into 4 categories each has 5 questions with total 22 questions specifically followed the research variables. The data of this research consisted of two kinds: primary data and secondary data. Primary data was gathered through use survey questionnaire and direct interview. Secondary sources will be collected from journal, textbook, articles, conference paper, documents and reports that published.

C. Objective

1. To assess user level of awareness in anticipating the risk.
2. To identify the relationship between human attitude perspective in maintaining user level of awareness among the institution.

D. Hypotheses

Hypothesis 1: *A role of responsibility of users in the institution complying with the requirements of the information security awareness positively affects her intention to comply.*

Hypothesis 2: *Performance from users as their human factors positively influences the information security awareness among environment.*

Hypothesis 3: *Adaptability from users as their human factors positively influences the information security awareness among environment.*

Hypothesis 4: *Learnability from users as their human factors positively influences the information security awareness among environment.*

E. Variables

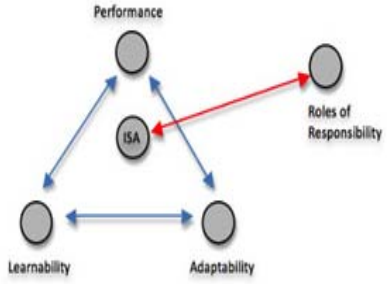

Figure 2. Variables Relationship.

In this study, the targeted variable which are:

1. Independent variable: 'Roles of Responsibility' is the value being manipulated or changed through process.
2. Dependent variables: 'Learnability', 'Adaptability' and 'Performance' are the value being influenced or being observed.

IV. RESULT

A. Data Analysis

Many separate data brings to specific information need to lead to same point before the analysis process takes part. The organizational of data approach after collecting data really important in getting general understanding interview process flow. Organization and categorization of data is the strategy will be used in data analysis by arrange the specific facts about the case in logical or chronological order and cluster the data into meaningful group which roles of responsibility, learnability, adaptability and performance. Recommendation and suggestion from volunteer become the great input in analyzing the pattern while the expert opinion enhance the quality of questionnaire. Around 7 respondents said that by taking ISA related course such as Cyber Law or IS Strategy and Policy will contribute to IIUM environment while 26 respondents eager to participate in IS trainings and program. Meanwhile, 25 respondents motivated to inform the other regards the importance of ISA and majority respondents (39) concerned about the improvement and evaluation of ISP in IIUM.

B. Survey Result

The questionnaire divided into 6 sections, which are respondent profile (1 question), roles of responsibility (5 questions), learnability (5 questions), adaptability (5 questions), performance (5 questions) and suggestion (1 questions). From 306 survey questionnaires was distributed to specific email, only 97 respondents (31%) fill them with their answer. They are 26 undergraduates (8%), 30 postgraduates (9%), 19 academics (6%) and 22 administrations (7%) respectively while the duration of data collection is 1 month. The data analysis of this research use simple correlation analysis of spearman's rho as well as significance test level (t).

TABLE I. SPEARMAN'S RHO CORRELATION: ROLES OF RESPONSIBILITY (2-TAILED)

ROLES OF RESPONSIBILITY	**Learnability**	**Adaptability**	**Performance**
Total: N= 97 Sig. (2-tailed)	0.849 000 t = 15.640	0.709 000 t = 9.87	0.836 000 t = 14.839
Undergraduate: N= 26 Sig. (2-tailed)	0.983 000	0.862 000	0.980 000
Postgraduate N= 30 Sig. (2-tailed)	0.700 000	0.709 000	0.976 000
Academic N= 19 Sig. (2-tailed)	0.7599 000	0.628 004	0.959 000
Administration N= 22 Sig. (2-tailed)	0.991 000	0.843 000	0.937 000

A. SIGNIFICANT AT THE 0.01 LEVEL (2-TAILED)

TABLE II. SPEARMAN'S RHO CORRELATION: INFORMATION SECURITY AWARENESS (2-TAILED)

Information Security Awareness	**Learnability**	**Adaptability**	**Performance**
Learnability		TOT: 0.775 UG: 0.994 PG: 0.738 AC: 0.788 AD: 0.816	TOT: 0.807 UG: 0.982 PG: 0.668 AC: 0.861 AD: 0.910
Adaptability	TOT: 0.775 UG: 0.994 PG: 0.738 AC: 0.788 AD: 0.816		TOT: 0.839 UG: 0.977 PG: 0.878 AC: 0.753 AD: 0.833
Performance	TOT: 0.807 UG: 0.982 PG: 0.668 AC: 0.861 AD: 0.910	TOT: 0.839 UG: 0.977 PG: 0.878 AC: 0.753 AD: 0.833	

B. TOT=TOTAL, UG=UNDERGRADUATE, PG=POSTGRADUATE, AC=ACADEMIC, AD=ADMINISTRATION

Hypotheses 2, 3 and 4 assumed that roles of responsibility from 4 different roles positively influence other variables like learnability, adaptability and performance. From the table I in line 1, the result of correlation analysis showed the result of coefficient 0.849 for learnability, 0.709 for adaptability and 0.836 for performance. They indicated the strong relation between roles of responsibility with those three variables. Moreover, the significance test showed 15.640, 9.87 and 14.839 respectively related to roles of responsibility that were more than 2.160 of coefficient 5% significance level, so, the 3 hypotheses were accepted.

Furthermore, the table II explained the relation from learnability, adaptability and performance specifically and dependently as the important element and requirement from information security awareness, which roles of responsibility should comply. The result indicated positive influence because it was on the range of 0.600 – 0.799 and 0.800 – 1.000, so the hypotheses 1 were accepted. The questionnaire comprises of roles of responsibility on opinion of appropriate responsibility, personal belongings, satisfactory level, knowledge sharing and importance of information security responsibility. Therefore, the learnability question consist of wireless policy, social engineering, approach in responding of password disclosure, computer virus description and XSS. Meanwhile, the adaptability question involve the anti virus selection, opinion on advancement technology, adaptability system description, malware and opinion on ISA. Lastly, the performance asked on identity theft, best practice in Malaysia, the first action if can't access account, the frequent act and performance reports.

V. DISCUSSION

In the context of awareness, person should have the adaptability as their preparation to fit with occurring changes or unexpected circumstances whereby affection or feeling from an individual has regarding an object become factor influenced. Thus, adaptability represents the emotion or motivation or even opinion on how to determine and

react efficiently towards unsecure of current situation that at further level, it implies at intention or feelings specifically. At last, it will lead to standard that person should have ISA after setting specific goals as priority. Therefore, performance concerns more on behavior contribute significantly and proactively on how to behave as the responses of the end users resulting from affection and cognition where it only implies to effectiveness of action. At the final step, when person can perform the right and fit action to encounter some issues, it will lead to ISA after specify the potential risk. Meanwhile, learnability is an individual's belief or knowledge about understandings an attitude object that is retrieving and extracting process as the way for improvement of current status to be better that before. It also leads to ISA after person identifies the weakness based on previous action.

Arguably, it could be some interrelation between the employee's preferred source and the employee attitude, which influence significantly towards the gaps between organization policy and strategy. While the solution proposed by many researchers to encounter ISA issues, the developing policy needs the combination of training, campaigning and reward system with the absent of one of them will significantly weakens the effectiveness of the policy [8]. ISA deals with the use of security awareness programs to create and maintain security-positive behavior as a critical element in an effective information security environment [6]. Human behavior that mainly lead to performance is recognized as a major problem in the implementation of information security practices in institution [1][3][7]. However, others claims that organization has no need to influence a user's behavior towards compliance with IS security instructions if the instructions are not available in an accepted format where regular assessment, evaluation of the effectiveness of the IS security awareness approaches and readjustment are much more necessary [8][9]. As such, researchers have called for the creation of ISC to help organizations to influence employee performance in order to better protect organizational information [15].

Meanwhile, it was identified through the survey that was developed that the majority of the learning on information security occurred where clear motivations, such as legislation and regulation existed [13]. People might distribute their feelings as the motivation to adapt with current situation or maintain their mood in the good state. This factor tends to be forgotten whereas it could appear as the critical factor when at particular time people has bad feelings or bad mood implicate home or internal issues lead to human careless in doing their duty. People might think they could maintain their interpersonal feelings in their working environment whereas the ability to adapt with the worst case scenario normally derived from experience or coming from setting of priority objective though it needs further analysis. Unfortunately, educating users about the threats and countermeasures in a dynamic environment like security requires time, resources and motivation [13] especially to raise the intention internally.

Security awareness is viewed as a multidimensional learning outcome, which comprises affective (feel), cognitive (understanding) and skill (acting) complementary. Cognitive perspectives focus on both trainee knowledge and the processes of knowledge acquisition, organization, and application [5]. All individuals must be trained on how to handle information carefully according to the guidelines and must be trained to become aware of the possible consequences of their actions [16]. Marks and Rezqui [8] suggested training and campaign as the best methods to increase understanding about ISA accommodates the uniqueness of specific location and durable of time. It is also important that the message and materials of IS training are the same regardless of who the trainer is [9] as well as regularly and continuity to increase the awareness in security performance.

VI. CONCLUSION

The engagement of IT knowledge-based institution such as library, human resource or IT division together will strengthen the goals of ISA initiative with detailed responsibilities and plan to obtain the target in developing ISP. However, ISP cannot guarantee a recipe for correct decisions but it provides an integrated perspective on goals, targets, and measures of progress. The main priorities in utilizing ISP pertain to translation on the vision, linking the vision to process and developing the plan to set the priorities and resources focus. Therefore, the evaluation from feedback and learning experience is required to measure the performance for the future function such as revise the plan and develop credible measure.

The policy to protect information in the university often not effective because the lack of awareness among student or staff due to less understanding the importance of information, the lack response in anticipating the current issues and less priorities in information security than the other. Three different human factors here aligned with the ABC model as the baseline produced three interconnected components that emphasize relationship between *knowing*, *feelings* and *doings* to determine the successful of ISP. The comprehensive study regards three aspects of human factors can measure the degree of awareness of environment to identify the further actionable step can be done for the purpose of improvement as well as process of aligning with other policy in relation of maintaining the competitive advantages. The exploitation to the important or critical information in the university can give negatively influence to the credibility of such university considering as the place for learning and practice for society. ISA should be as the first priority in the development of ISP by executive level due to the its important function as the identification, measurement and stimulus of influence, contribution and effect.

REFERENCES

[1] Bulgurcu, B. "Motivations in Information Security Policy Compliance: An Empirical Study of Information Security Awareness and Perceived Fairness," *Americas Conference on Information Systems*. San Francisco, California August 6th-9th 2009.

[2] Fung, C. C., Khera, V., Depickere, A., Tantatsanawong, P., & Boonbrahm, P. "Raising Information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand". *2nd IEEEInternational Conference on Digital Ecosystems and Technologies (IEEE DEST 2008)*, Phitsanulok, pp 375-380.

[3] Harrison, D. A., Newman, D. A., & Roth, P. L. "How important are Job Attitudes? Meta-Analytic Comparisons of Integrative Behavioral Outcomes and Time Sequences". *Academy of Management Journal*, *49* (2), 2006, pp. 305-325.

[4] ISF. (2005). *The standard of good practice for information security* (Version 4.1). Information security forum.

[5] Kraiger, K., Ford, J.K., and Salas, E. Application of Cognitive, Skill-Based and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology*, *78* (2), 1993, pp 311-328.

[6] Kruger, H.A., & Kearney, W. D. "A Prototype for Assessing Information Security Awareness". *Computers & Security, 25* (4), 2006, pp 289-296.

[7] Lim, J.S., Ahmad, A., Chang, S., & Maynard, S. "Embedding Information Security Culture Emerging Concerns and Challenges". *PACIS 2010*.

[8] Mark. A., & Rezgui, Y. "A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing". *International Conference on Management and Service Science (MASS)* 20-22 Sept. 2009, Wuhan, pp 1-7.

[9] Pastor, V., Diaz, G. and Castro, M. "State-of-the-art Simulation Systems for Information Security Education, Training and Awareness". Education Engineering (EDUCON) 14-16 April 2010, Madrid, pp1907-1916.

[10] Rezgui, Y., & Marks, A. "Information security awareness in higher education: An exploratory study". *Computers & Security*, 27 (7-8), 2008, pp 241-253.

[11] Siponen, M.T. "A conceptual foundation for organizational information security awareness". *Information Management & Computer Security, 8* (1), 2000, pp 31-41.

[12] Tolnai, A., & von Solms, S. "Solving Security Issues using Information Security Awareness Portal". *International Conference for Internet Technology and Secured Transactions (ICITST)* 9-12 Nov. 2009, London, pp 1-5.

[13] Thalib, S., Clarke, N. L., & Furnel, S. M. "An Analysis of Information Security Awareness within Home and Work Environments". *International Conference on Availability, Reliability and Security (ARES)* 15-18 Feb. 2010, Krakow, pp 196-203.

[14] Takemura, T. "A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey". *American Journal of Economics and Business Administration, 2* (1), 2010, pp 20-26.

[15] Veiga, A. D., & Eloff, J. H. P. "A Framework and Assessment Instrument for Information Security Culture". *Computers & Security, 29* (2), 2009, pp 196-207.

[16] Wipawayangkool, K. "Security Awareness and Security Training: An Attitudinal Perspective". *SWDSI 2009*. 266-273.