Implication of Human Attitude Factors toward Information Security Awareness in Malaysia Public University

Abdul Rahman Ahlan[1], Yusri Arshad[2] and Muharman Lubis[3]

Kulliyah of Information Communication Technology,
International Islamic University of Malaysia (IIUM), Malaysia
arahman@iium.edu.my[1]
yusriarshad@gmail.com[2]
muharman.lubis@gmail.com[3]
Corresponding Author: muharman.lubis@gmail.com

Abstract

Without a doubt, the whole world faces many challenges regarding hacker or cracker exploitation; and spammer in various sector such as Internet security, software privacy, email, etc. While Malaysian government attempted to establish several cyber laws in order to encounter the problem, mainly as the guidance for technology user's purpose, the danger in information exploitation still arise. The important factor that supports the successful of these policies implementation resides on how to raise the awareness among community. This process will give significance contribution to the effectiveness of policy implementation by its continuity through the communication chain and regularly information distribution. Government can't overrule the importance of university policies in building the awareness among student at beginning phase. Therefore, some factors need to be identified first, from which level that might influence positively the awareness in university. It has the function to measure the level of awareness for the improvement and performance purpose. However, the problem will always occur in terms of evolving the human mind in utilizing technology services, which put information security susceptible to attack and there is no standard regulation to ensure that human attitude involved delivering the secure and safety result. So, we can conclude that human error could be as greatest risk if current organization's policy doesn't have the capability to control and manage it accordingly and frequently.

Keywords: Information security awareness, information security policy, human attitude, responsibility

1. Introduction

There are several issues that should be addressed relate to information security namely awareness, strategy, procedure, policy and so forth. Therefore, the main issues regards information security awareness (ISA) should be as the priorities due to achieve significant growth (Mark & Rezqui, 2009; Thalib et al., 2010). Some challenges might involve on human attitude, which is really difficult to measure affected by the influence of some aspects like culture, motivation, value, mindset, etc. (Kruger & Kearney, 2006). The development of specific strategy should overcome the potential challenge and threats coming from inside and outside organization in order to synchronize with organization's policy. 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. Then, it is also necessary to identify the background of end users to understand the source of the risk and view the relation or effect of the target user's vulnerabilities and weakness towards organization policy.

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 internally and externally. 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 environment and limitations and concludes by discussing further research directions in the area.

1.1. Problem statement

Evidences from literature indicated that human careless could be the greatest threats for organization in terms of information security process (Pasto et al., 2010; Kraiger et al., 1993; North et al., 2010). There hasn't been many research conducted in the direction of measuring level of awareness from end user in information security in the practical way. Thus, the paper will investigate the relation between policy with the human attitude such as behavior, attribute, mindset, understanding and response as factors that influence the level of awareness inside the organization. Those factors will be classified based on the significance of its contribution towards one another and especially to ISA. The choice to do an investigation on the ISA is seen important that will lead to develop suitable strategy to enhance university capability and trust. It has to do to accommodate the need of regular improvement and bridge academic and practical perspective.

1.2. Scope of research

The study will scope down the categories into four participants; academic, admin staff, undergraduate and postgraduate student of specific public university. It limits the geographical boundaries in Malaysia and specific Public University as the sample for generalization. In this study, ISP is defined as staffs' and students' general knowledge about information security involves regulation and procedure of information protection made by the university. Meanwhile, human attitude is defined as the perception, association, intention, response and action relate to intellectual, emotional and spiritual of each individual. Roles responsibility is defined based on unique position of people that will be investigated in public higher education to identify whether the difference in circumstances lead to specific results.

1.3. Significance of research

The significances of this study are the contribution to the community through its implications, the importance of the theory and its limitation to hypothesis. Human attitude is a part of the consideration that will be investigated to develop a suitable university's policy that will accommodate organization needs in understanding the difference on intention and fluctuation in the environment towards information security. Hopefully, the study will give benefits especially in public university concern on the importance of managing human resource to inbuilt awareness for protecting information so the risk of exploitation by wrong hands will be minimized.

2. Literature Review

2.1. Theoretical Background

Information security issue already become top priorities in various institutions and strongly related to the concept of risk. According to the Information Security Forum (ISF) (2005), 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 (2000) defined security awareness as "*a state where users in an organization are aware, ideally committed to, of their security mission*".

Study of Mark and Rezqui (2009) provide the comparative study of factor affecting decision making in ISA, with emphasizing the lack of internal behavior in the organization, direct relationship between application and IS assets towards the awareness. They also proposed sequential design theory for IS awareness to establish the concrete and suitable policy consist of campaigning, reward and training complementary. Accordingly, two important factors need much consideration in raising awareness are how organization influences significantly of end user's behavior and how the organization has the regular assessment or evaluation to measure the effectiveness of IS awareness policy inside the organization. Interestingly, they argued that current research in IS awareness most of the

approaches are neither based on theory, nor empirically validated in practice whereby did not deliver practical and specific guidance to practitioners regarding the implementation of the framework. Meanwhile, creating the alignment of goals, policies and procedures is not effective if there is no proper action to communicate, publish and understood by the community, so the extraction of environment's response is really essential in developing the suitable IS security policies that align with organization goals and procedures.

Another initiatives by Fung et al. (2008) in their pilot study suggest the using of games and simulation to increase the awareness and knowledge level of student in terms of information security rather than just using simple training session. It was evidence by the analysis study of two group (Fung et al., 2008) which had training session and games simulation separately indicated the huge difference on how the games' group values assets, purpose and privacy higher than training's group although the benefits of training was quite significant in setting up the policy and procedure but it lacked the in depth understanding and awareness of information security importance. The effectiveness of this method also proven by higher percentage with 50% respondent on games and simulation group's answered that they could apply the knowledge and idea in real life while in the training's group showed less than that.

Another interesting study comes from Talib et al. (2010) mentioned that learning process of information security knowledge practice in workplace comes from informal source such as website, search engine and informal discussion with the experts or colleagues. It was directly indicated that majority existing organization policy standards was not effective to raise awareness among the employee. These proportion have huge impact to organization capability that show majority employee preferred to learn by themselves or through another outside experts. Besides that, the issues with internal process also really extreme with assumption of huge estimation in human error which contributed higher than external process as the threats in term of information security leaked like configuration management, administrations careless and miscommunication among the admin.

Therefore, study by Tolnai and von Solms (2009) 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 (Fung et al., 2008; Pasto et al., 2010; Thalib et al., 2010). 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.

2.2. Affect, Behavior and Cognition (ABC) Model

According to Information Security Management Handbook (Micki & Harold, 2007), ABC model also known as "Tripartite model" presents attitude as three separate measurable components, which are:

1. ***Affect:*** *emotional aspect, feelings toward an object or subject.*
2. ***Behavior:*** *derived from the fact that it serves as a feedback mechanism.*
3. ***Cognitive:*** *thoughtful, thinking aspect, opinions be developed based widely solely on insightful.*

Attitudes can be influenced by various factors externally in the process of interaction in the environment. Some claims mentioned about culture might influence performance in protecting organizational information (Veiga & Eloff, 2009). In general, human attitude towards performance depends on ability, motivation and working conditions (Bartol & Martin, 1994). Meanwhile, some claims accentuates on how to embed the culture in the environment in a holistic manner. It was expected to include senior management support and involvement to instill awareness through mandatory training based on clear assignment of responsibility and constant enforcement of security policies and procedures (Lim et al., 2010). It is very important that the people responsible for raising security awareness should regard carefully the methods for enforcement positively and truly right. They also should be capable in term of justifying them if challenged as necessary point of departure for the persuasion method in strengthen ISA among the community (Siponen, 2000).

There are important and significant differences between understanding of information security and ethical computer use among students in public universities and private universities. The way of individuals is taught and the way the students learn will create a large variance in each culture's perspective (North et al., 2010). So, the perception and interpretation of some terminology and lexicon is more subjective on their perspective. The lack of consistency on definition simply made other predicted approach and process only suitable to certain cases. The attitudes of staff and student have been identified as a key factor in the protection of organizational information. As such, many researchers have called for information security culture (ISC) to be embedded into organizations to positively influence human attitude towards protecting organizational information (Veiga & Eloff, 2009; Siponen, 2000; North et al., 2010).

3. Aim and Purpose

3.1. Research Goals

1. To assess level of awareness from Public University end users to anticipate risk based on roles of responsibility.
2. To develop the comprehensive university policy to protect information based on understanding of human factor perspective (learnability, adaptability and performance).

3.2. Research Questions

1. What are the current information security awareness challenges and threats in Public University?
2. How the human attitude can influence university environment in enhancing the information security awareness?

4. METHODOLOGY

This study will use quantitative methodology with 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 limited to just once. The questionnaire will be divided into 4 categories each has 5 questions with total 22 questions specifically followed the research variables.

4.1. Sampling and Data Collection

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, 300 users involve 200 students and 100 staffs 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.

4.2. Research Variables

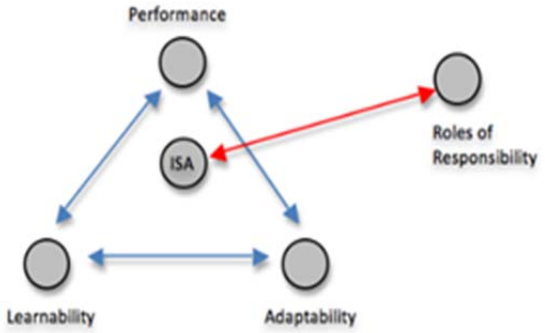

Figure 1. Variables Relationship

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.

5. HUMAN ATTITUDE PERSPECTIVE

The ABC model is used as the baseline while three equivalent dimensions was developed and adjusted as the ability from end users to connect with ISA into '***Adaptability***', '***Performance***' and '***Learnability***'. Adaptability is equivalent with affect as the ability to show feelings, adjust mood and maintain motivation and response towards a subject or object drive some critical condition. Performance is equivalent with behavior as ability to react towards certain situation or condition and perform the suitable approach and measurement to show its potential capability and capacity. Learnability is equivalent with cognitive, means the ability to think critically and logically based on experience as well as to extract or retrieve the useful information into knowledge from resources concurrently.

5.1. Roles 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 (Wipawayangkool, 2007). Meanwhile, Harrison et al.'s presented attitude-engagement model associates overall job attitude with individual effectiveness (2006). Therefore, Bulgurcu (2006) emphasized the importance of the role of an employee's ISA and her perceived fairness of the requirements of the ISP. Furthermore, users prioritize other work tasks in front of information security while main problem regarding users' role in the information security work is ascribable to their lack of motivation and knowledge regarding information security and related work (Albrechtsen & Hoyden, 2009). 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 (Takemura, 2010) finds 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.

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

5.2. Performance

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

(Mark & Rezqui, 2009). Logically, the appreciation for the employees' action by giving the rewards or praise based on their contribution can increase the performance significantly. It is expected to pull other employee to maintain their well performance and compete with each other in the form of improvement. 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 (Kruger & Kearney, 2006). Human behavior that mainly lead to performance is recognized as a major problem in the implementation of information security practices in institution (Harrison et al., 2006; Bulgurcu, 2006; Lim et al., 2010). 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 (Mark & Rezqui, 2009; Rezqui & Marks, 2008). As such, researchers have called for the creation of ISC to help organizations to influence employee performance in order to better protect organizational information (Veiga & Eloff, 2009).

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

5.3. Adaptability

Good leadership skills and a healthy organizational culture complementary are important factors in the creation of a basis for security awareness, as they affect the achieving of intrinsic motivation and intention and also perceived usefulness (Davis, 1989). 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 (Thalib et al., 2010). 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 (Thalib et al., 2010) especially to raise the intention internally. Prioritizing what should be achieved and obtained through specific criteria expected develop the good intention of relevant people to maintain the awareness by giving suggestion or opinion among them, or it might focus and concern to improve own selves at beginning.

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

5.4. Learnability

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 (Kraiger et al., 1993). 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 (Wipawayangkool, 2007). Marks and Rezqui (2009) 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 (Rezqui & Marks, 2008) as well as regularly and continuity to increase the awareness in security performance. Therefore, the understandings in the form of learnability become important when facing the fast changes and unexpected event. The readiness of people can be set through the preparation. The understanding can be measured by comparing the previous case on the impact, effect and implication of exploiting information or when the organization neglecting and underestimating the important of information. When people don't have certain knowledge to control or handle computer device, it leads to potential risk and failures, this logical points also could be implicated to information security awareness as well.

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

6. 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.

Information security failures can be costly to any institution. Losses may be suffered as a result of the failure or the cost incurred for recovery, followed by more cost to secure systems and prevent further failures. Meanwhile, many managers and employees also tend to think of information security as a second priority compared with their own efficiency or effectiveness matters regards direct and material impact on the outcome of their work. In terms of awareness, the obligation belongs to the specific role responsibility of staff and student for example one's duty as laid down by the university and one's moral concern to do the right thing. It is possible to achieve moral responsibility if the security actions of an organization are seen as morally acceptable and desirable in the eyes of the staffs and students through proper policy and procedure (Albrechtsen & Hoyden, 2009). In the long run, this obligation should be retrieved internally, within the individual (Takemura, 2010). However, if obligation is so weighty leads to prescriptive states, can cause greater risks in the form of negative implications such as pressure or irritation, which reduce work efficiency and even produce resistance or unethical or other unwanted behavior (Siponen, 2000).

To increase understanding awareness issue, two categories can be outlined, framework and content (Siponen, 2000). The combination of beliefs, habits and behaviors in form of attitude influence on how such community reacts to a policy and regulation. Unlike personality, attitudes are expected to change through experience. Commonly, attitudes can be changed through persuasion and we should understand attitude change as a response to communication (Micki & Harold, 2007). The establishment of training also be encouraged to ensure that users are informed and can be accounted liable for IS misconduct (Rezqui & Marks, 2008). The risk management should be aligned for ensuring selection of proper management that support by ISA to improve the implementation capabilities as well as assistance in identifying, assessing and managing the risk process. Supports from executive is really useful to strengthen the ISP, securing staff commitment and enhance student contribution, also critical in relation with the human attitude fluctuation, that can make bad image or outlooks in certain people’s perspective, in some case it could threaten the work performance.

Study from Rezqui and Marks (2008) gave the recommendation to establish ISP in the university, which consisted 6 points, can be consideration. Therefore, 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. Meanwhile, the isolation program such as training, seminar or workshop is not enough to increase or maintain the awareness between employee and complementary program are the answer to overcome these issues. At last, the further step for measuring and assessing the

awareness level is the ISA level maturity model that Public University can benchmarking their own implementation as the standards of stage level awareness based on specific criteria derived from three interconnected components, which are learnability, performance and adaptability. Such evaluation to the implementation of ISA level maturity model will enhance the readiness of Public University to face information security exploitation internally. Other institution with considering the ISM, ISC and ISP as well also can adopt the standard of maturity model in IS awareness.

8. Conclusion

In conclusion, 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 its important function as the identification, measurement and stimulus of influence, contribution and effect.

References

Albrechtsen, E. & Hovden, J. (2009). The Information Security Digital Divide between Information Security Managers and Users. *Computer and Security, 28* (6), 476-490.

Bartol, K. M., & Martin, D. C. (1994), *Management* (Second international edition). New York, NY: McGraw-Hill.

Bulgurcu, B. (2009). 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.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13* (3), 319-40.

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

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

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

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

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

Leidner, D and Kayworth, T. (2006). The Role of Culture in Knowledge Management: A Case Study of Two Global Firms. *International Journal of e-Collaboration,* 2 (1), 17-40.

Lim, J.S., Ahmad, A., Chang, S., & Maynard, S. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. *PACIS 2010*.

Mark. A., & Rezgui, Y. (2009). 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.

Micki, K., & Harold, F. T. (2007). *Handbook of Information Security Management*. CRC Press LLC.

North, M., Perryman, A., Burns, S., & North, S. (2010). A Comparative Study of Information Security and Ethics Awareness in Diverse University Environments. *JCSC, 25* (5), 223-230.

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

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

Thalib, S., Clarke, N. L., & Furnel, S. M. (2010). 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.

Tolnai, A., & von Solms, S. (2009). 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.

Takemura, T. (2010). 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), 20-26.

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

Wipawayangkool, K. (2007). Security Awareness and Security Training: An Attitudinal Perspective. *SWDSI 2009*. 266-273.