VOL. 10, NO. 16, SEPTEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

# CONCEPTUAL STUDY TOWARDS INFORMATION SECURITY MODEL FOR E-LEARNING STAKEHOLDERS

Najwa Hayaati Mohd Alwi[1], Ip-Shing Fan[2] and A. H. Azni[3]
[1, 3]Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, Malaysia
[2]School of Applied Sciences, Cranfield University, Bedfordshire, United Kingdom
E-Mail: najwa@usim.edu.my

**ABSTRACT**

This paper presents the conceptual model of the Information Security Vulnerability for E-learning Stakeholders. This model is the derived from literature reviews and multi method studies. The proposed model incorporates the dimensions, components which bringing out the relation of people's behavior and information security. The model depicted the relationship of dimensions related in the management of information security of stakeholders in e-learning by addressing people's behavior and their cultural view. The model serves as an integrative structure to understand and define the stakeholder's cultural view in securing the e-learning environment.

**Keywords:** information security, e-learning, culture, behavior, stakeholder.

## INTRODUCTION

The dependence of E-learning to the Internet or, specifically, mostly via web applications exposed the e-learning environment to the information security threats. E-learning is different from other e-services in the applications used, the procedures and the stakeholder behavior which shaped the environment in e-learning. Issues of reliability of the system in course material, data privacy in the grading result, non-repudiation and misuse of Learning Management System (LMS) are example of social technical security issue that is specifically related to people.

People's behavior is not specifically addressed in the security control mechanisms, though they are one of the components of IT systems and a source of information security threats. Information Security Management (ISM) standard has been deployed from top to bottom and a security policy is blanketed for all users.

Users need to follow policy, procedures and others activities to ensure the security principle: confidentiality, integrity, and availability [1] is achieved. Users are expected to be the security controllers themselves. However people also can be the vulnerabilities where threat can occur, for instance: password sharing, non-repudiation, and malware infection. The current trend of social engineering manipulates people's level of security awareness, for example phishing that allures users into giving information. This suggests that individual action can cause security threats.

This paper will explain the developed model with the aim to provide fundamental dimensions in the management of information security for stakeholders in e-learning. The model serves as an integrative structure to understand and define the stakeholder's cultural view in securing the e-learning environment. This will help e-learning provider manage the stakeholders and ensure the information security management take place.

In addition, the proposed model provides generic dimensions to ISM in e-learning, which in turn is expected to assist in increasing the awareness and responsibilities among stakeholders towards securing the e-learning environment. This model also contributes in providing control to avoid the threats, usually known as preventive control. Preventive control is taking measures that would prevent the information from being damaged, altered, or stolen by identifying the possible threats and implementing the suitable control based on cultural view of stake holders. This model complemented the critical successful model by [2-6], and achieving the successful of security standards such as ISO/IEC27002.

The following sections will describe the literature review, and methodology of development. This paper will further concentrate on elaborating the dimensions structure and the components for each dimension of the proposed conceptual model.

## LITERATURE REVIEW

Information security includes protection of any threats to avoid the fabrication, modification, interruption and interception of information [7]. Information security threats are caused by persons who intentionally or unintentionally interfere with the normal business process. A variety of controls are in the market to ensure the continuity of business and minimize the loss. ISM provides standards - ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 as guidance to manage information security. The standards set outline the policy, training and education to improve the security culture among users. Technological factors are not the merely contributing factor of information security controls effectiveness. There is also a need to understand the security challenges in implementing IT security in organizations [6], [8].

### E-learning Stakeholders

E-learning is the implementation of technology to support the learning process [9]. The successful of the implementation depends on community of people to make it work. There are different stakeholders in e-learning environment who must play their roles to ensure the


successful of e-learning implementation. The main stakeholder groups in the context of higher education have been complied by [10]. In a way, the e-learning community can be classified as two groups: The Supply group and Demand group. The Supply group is the learning provider that offers the e-learning environment. This group consists of top management, IT department staff, e-learning service centre and other staff that support the e-learning development and delivery process. The demand group consists of end-users that will benefit the most from this environment. They are lecturers and students.

**Security in E-learning**

Previous studies have shown that there is a barrier to the wide-spread adoption of online education [11]. It is claimed that the reason behind this barrier is not only the high cost or further preparation has still to be done but also the security aspect which is something that is completely intangible in the cyber world [12]. It has been said that e-learning institutions try to address privacy and security, however the standards are implanted superficially [13].

There have been some studies on the requirement of security in e-learning [13-16] and technical guides on web based system security in e-learning [17-18]. However, none have considered that different cultural views among stakeholders may bring different security threats.

E-learning systems are exposed to security risk [19]. Thus, security in e-learning is significant. Among the risk are interruption, interception, modification and fabrication of data and activities. There is four principles security requirements need to be emphasize in e-learning. These are confidentiality, integrity, availability and non-repudiation. The details of these principles are explain in [20].

The discussion on security in e-learning in literature has placed the responsibility to secure e-learning on the top management and the IT personnel whereas the security should be an organizational culture to focus. It is responsibilities of everyone in an organization.

**Grid and Group Culture Theory**

Organizational culture can be discussed from many perspectives. This paper applies a well-known theory - Grid and Group Cultural Theory or also known as Cultural Theory (CT). This theory reflects the level of an individual in an organization and addressed the changes both within and between dimensions as well as dynamism [21]. Additionally CT has been used to analyze environmental and technological risks differences in society [22-24].

CT framework build from two dimensions: Grid and Group. The Grid dimension implies the level of a social context is regulated and restrictive in regard to the individuals' behavior. Whereas the Group dimension refers to an individual as member of bonded social units, how engaging the group's activities are on the individual [25]. Four different cultural views with distinct ways of life or worldviews are derived [26]. Table-1 represented grid and group relationship with the four ways of life:

**Table-1.** Grid and group cultural view.

| Cultural view | Grid | Group |
|---|---|---|
| Fatalism (FTL) | Strong/High | Weak/Low |
| Hierarchism (HIE) | Strong/High | Strong/High |
| Individualism (IND) | Weak/Low | Weak/Low |
| Egalitarianism (EGA) | Weak/Low | Strong/High |

Fatalism is a view held by people with a strong Grid and low Group, indicating apathy and isolation. Fatalist prefers to be unaware of dangers, as they perceive somehow that nothing much they can do. They feel obliged to accept all rules and regulations imposed, and are not liable to breach security controls for their personal gain. This is due to they accept that they have little or no power to influence the course of events in their favor [24]. However fatalism views lead to the development of ignorance character, which increases the risks of unintentional threats.

On the other hand, Hierarchism is a view held by people who are strong in Grid and Group dimensions, indicating strong control and power. Hierarchists usually trust experts and respect the rules [22]. However they also are likely to break rules or act uncooperatively to a policy as a group [23].

Another culture view is Individualism. This is a view held by people with both low Grid and low Group, indicating independence and self-reliance. Individualists are known as people with reluctance to acknowledge rules particularly if these rules observed as hampering their freedom [22].

The last culture view is Egalitarianism where this is a view held by people with a low Grid and Strong Group, indicating teamwork and cooperation. With intense sense of equality [24] egalitarians have more difficulties in accepting role differentiations. However they support decision-making processes that encourage public participation.

**ISM Components**

The ISM components are policy, process and procedures and organization structure. [27].Each component defines the activities or actions that need to be carried out, its' relationship with cultural view elements and subsequently with the stakeholder. Table 2 listed the activities related to e-learning for each components of ISM.

**Table-2.** ISM components.

| ISM Components | Activities |
|---|---|
| Policy | 1. Define the security requirement for e-learning considering the cultural view of stakeholder.<br>2. Testing the policy using actual stakeholder and system.<br>3. Support the policy by publishing in the website and provide a talk or to expose policy to the community with considering the stakeholder cultural view.<br>4. Evaluate the policy frequently ensuring it address the stakeholder cultural view. |
| Process and procedures | 1. Define the security requirement for processes and procedures considering the cultural view of stakeholder.<br>2. Testing process and procedures e-learning using actual stakeholder group.<br>3. Support the process and procedures, e-learning with documents guide and training considering the stakeholder cultural view.<br>4. Evaluate the process and procedures e-learning frequently so that it keeps up to date with stakeholder cultural view. |
| Organization structure | 1. Define the roles, job scope and the level of security privilege.<br>2. Structure should not be hierarchy but more to cross communication.<br>3. Support and provide training according to the group considering the stakeholder cultural view. |

**Methodology of Development**

This section will explain briefly on how the model is developed. This research conducted a literature review and two stages of data collection and analysis as depicted in Figure-1. Six steps conducted in both stages. The methods used in these data collections and analysis phase includes literature review, online questionnaire, interview, and document analysis.

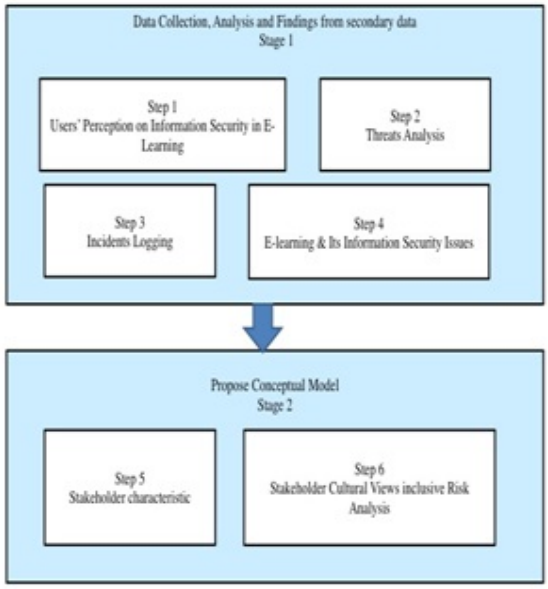


**Figure-1**. Data collection, analysis and findings stages.

The first stage as presented in Figure 1. attempts to understand and identify the requirement of security in e-learning [27] which resulted in the identification of the dimensions for ISM model. Four studies have been carried out in the first stage. When Step 1 was conducted to explore the security in an e-learning situation, the finding has significantly pointed to the people issues. Users are not aware of the threats and security situation in e-learning. Step 2 has looked into the relationship between people, threats and countermeasures. It has provided knowledge on the roles and responsibilities of actors in the security issue for each application in e-learning, the situation and possible threats of e-learning. Identifying the threats specific to e-learning can help the providers to plan suitable countermeasures [28]. Step 3 used known incidents to understand the types of attack, and people are an important source of attack for e-learning. These steps have led the researcher see that people need to be addressed more visibly in the ISM standard and guidelines. Individual factors and how people perceive risk is a part of the explanation for users' view on information security [29]. The findings from Steps 4 have reflected the e-learning situation of the public universities and gained face to face dialogues to corroborate with the other studies [27, 30]. The output of the first stage identified insider as one of the main threats and focus studies in the second stage, which is to understand cultural views and their impact on e-learning.

Figure-1 depicted as well the Stage 2- Proposing the conceptual model. Two steps have been carried out in the second stage. These activities were conducted to investigate whether different stakeholder are susceptible to certain types of security threats or if security threats are particular to different categories of stakeholders. There are two studies conducted in this stage. The outputs of second stage correlate the cultural view with different types of

responses to threats. The correlation between cultural views of stakeholders in e-learning and type of responses of security threats proposed model of ISM for e-learning [20].

**Model Constructs and Details**

**Design Approach and Structural Dimension**

Figure-2 depicted the four dimensions of proposed conceptual model of E-Learning Stakeholders Information Security together with the relationships. The correlation between each dimension in the model was derived from the findings of Step 6 (as shown in Figure-1) conducted.

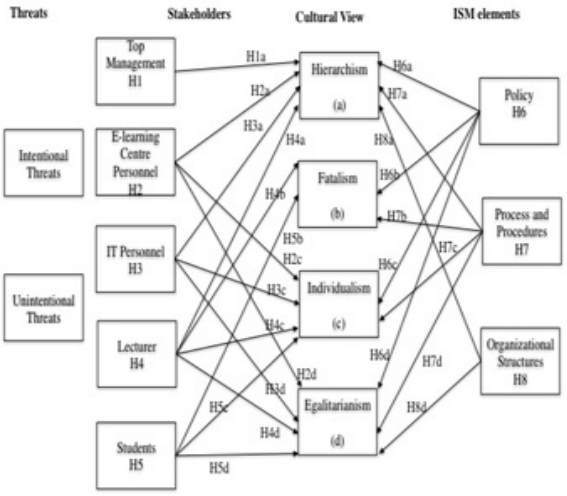


**Figure-2.** Proposed conceptual model of E-Learning stakeholders information security model.

The model incorporates the dimensions that bring out the relationship between people's behavior and information security. The dimensions are Threats, Stakeholders, Cultural View and ISM Elements. Each dimension is positioned in a column that contains the components. The dimensions are presented next to each other reflecting the adjacent correlation. Threats are related to stakeholders. While stakeholders contribute threats and at the same time they are influenced by cultural view they hold. Therefore stakeholders dimension is position between threats and cultural view dimensions. In the meanwhile, cultural views posed by stakeholders and can influence the suitable control to be engaged to stakeholders. Therefore cultural view column positioned between stakeholders and ISM elements.

Threats dimension consists of two components describing the type of threats possible in e-learning. It includes the intentional and unintentional threats. It is common and possible to receive threats from malicious human with intentions to bring harm.

The stakeholders dimension is basically both supply and demand group that form the e-learning community. This dimension consist of five components namely Top Management, E-Learning Centre Personnel, IT Personnel, Lecturer and Student.

These stakeholders have different attribute such as roles and behavior that generate their own cultural view. From the proposed model, the hypothesis that shows the relationship between the components is shown in Table-3.

**Table-3**. Hypothesis of proposed conceptual model.

| Hypothesis | Relationship |
|---|---|
| H1a | Top Management has a positive relationship with hierarchism cultural view |
| H2a | E-learning Centre Personnel has a positive relationship with Hierarchism cultural view |
| H2c | E-learning Centre Personnel has a positive relationship with Individualism cultural view |
| H2d | E-learning Centre Personnel has a positive relationship with Egalitarianism cultural view |
| H3a | IT Personnel has a positive relationship with Hierarchism cultural view |
| H3c | IT Personnel has a positive relationship with Individualism cultural view |
| H3d | IT Personnel has a positive relationship with Egalitarianism cultural view |
| H4a | Lecturer has a positive relationship with Hierarchism cultural view |
| H4b | Lecturer has a positive relationship with Fatalism cultural view |
| H4c | Lecturer has a positive relationship with Individualism cultural view |
| H4d | Lecturer has a positive relationship with Egalitarianism cultural view |
| H5b | Students has a positive relationship with Fatalism cultural view |
| H5c | Students has a positive relationship with Individualism cultural view |
| H5d | Students has a positive relationship with Egalitarianism cultural view |
| H6a | Elements policy as a countermeasure has a positive relationship with Hierarchism cultural view |
| H6b | Elements policy as a countermeasure has a positive relationship with Fatalism cultural view |
| H6c | Elements policy as a countermeasure has a positive relationship with Individualism cultural view |
| H6d | Elements policy as a countermeasure has a positive relationship with Egalitarianism cultural view |
| H7a | Elements process and procedures as a countermeasure has a positive relationship with Hierarchism cultural view |
| H7b | Elements process and procedures as a countermeasure has a positive relationship with Fatalism cultural view |
| H7c | Elements process and procedures as a countermeasure has a positive relationship with Individualism cultural view |
| H7d | Elements process and procedures as a countermeasure has a positive relationship with Egalitarianism cultural view |
| H8a | Elements organizational structures as a countermeasure has a positive relationship with Hierarchism cultural view |
| H8d | Elements policy as a countermeasure has a positive relationship with Egalitarianism cultural view |


## CONCLUSIONS

This paper proposed a conceptual model for ISM e-learning that highlighted the cultural view of people. The proposed conceptual model of E-Learning Stakeholders Information Security Model depicted the relationship of dimensions related in the management of information security of stakeholders in e-learning. By addressing people's behavior and their cultural view, a more prudent and robust security policy can be designed particularly to counter threats that employ social engineering techniques that manipulate people's behavior and perceptions. Instead of using the technological control, this model provided insight into security control by addressing the peoples' cultural view. In future a testing approach or tools to enable integration to address the cultural view in controls in current ISM practice can be designed.

## REFERENCES

[1] Gollman, Dieter, "Computer Security", Wiley Interdisciplinary Reviews: Computational Statistics, 2, no.5, (2010), pp 544-554.

[2] Kankanhalli A., Teo H. H., Tan B. C. Y. and Wei K. K. 2003. "An integrative study of information systems security effectiveness", International Journal of Information Management, Vol. 23, No. 2, pp. 139-154.

[3] Da Veiga A., and Eloff J. H. 2010. "A framework and assessment instrument for information security culture", Computers & Security, Vol. 29, No. 2, pp 196-207.

[4] Alnatheer M. A. 2014. "A Conceptual Model to Understand Information Security Culture", Int. J. Soc. Sci. Hum., Vol. 4, pp 104-107.

[5] Alhogail A. and Mirza A. 2014. "A Framework of Information Security Culture Change", Journal of Theoretical and Applied Information Technology, Vol. 64, No.2.

[6] Hassan N. H. and Ismail Z. 2015. "A Conceptual Model Towards Information Security Culture in Health Informatics", In The Malaysia-Japan Model on Technology Partnership, Springer Japan, pp. 187-196.

[7] Stallings W. 2007. "Network Security Essentials: Applications and Standards", Prentice Hall.

[8] Werlinger R., Hawkey K. and Beznosov K. 2009. "An integrated view of human, organizational, and technological challenges of IT security management", Information Management & Computer Security, Vol. 17, No. 1, pp. 4-19.

[9] Johnson R. D., Hornik S. and Salas E. 2008. "An empirical examination of factors contributing to the creation of successful e-learning environments", International Journal of Human-Computer Studies, Vol. 66, No. 5, pp. 356-369.

[10] Wagner N., Hassanein K. and Head M. 2008. "Who is responsible for E-Learning Success in Higher Education? A Stakeholders' Analysis", Educational Technology & Society, Vol. 11, No. 3, pp. 26-36. 11.

[11] Allen E. and Seaman J. 2007. "Online Nation Five Years of Growth in Online Learning", Sloan Consortium, United States.

[12] Zhang D. and Nunamaker J. F. 2003. "Powering E-learning in The New Millennium: An Overview of E-learning and Enabling Technology", Information Systems Frontiers, Vol. 5, No. 2, pp. 207-218.

[13] El-Khatib K., Korba L., Xu Y. and and Yee G. 2003. "Privacy and security in E-learning.", International Journal of Distance Education Technologies, Vol. 1, No. 4, pp. 1-19.

[14] Adams A. and Blandford A. 2003. "Security and Online Learning: to Protect or Prohibit", in Ghaoui, C. (ed.) Usability Evaluation of Online Learning Programs, Information Science Publishing, London, pp. 331-359.

[15] Furnell S. M. and Karweni T. 2001. "Security issues in Online Distance Learning", VINE: The Journal of Information and Knowledge Management Systems, Vol. 31, No. 2.

[16] Tsiantis L. E., Stergiou E. and Margariti S. V. 2007. "Security Issues in E-learning Systems", Computation in Modern Science and Engineering, Volume 2, Part B (AIP Conference Proceedings, Vol. 963, pp. 959-964.

[17] Cummings C. S., Shi H., Shang Y. and Chen S. 2005. "A Flexible Authentication and Authorization Scheme for a Learner Information Management Web Service", International Journal of Information Technology and Decision Making, Vol. 4, No. 2, pp. 235-250.

[18] Jalal A., Zeb M. A. and Peshawar P. 2008. "Security Enhancement for e-Learning Portal", International Journal of Computer Science and Network Security, Vol. 2, No. 4, pp. 236.

[19] Weippl E. R. 2005. "Security in E-learning", Advances in Information Security, vol. 16 ed, Springer Science + Business Media, Inc, USA.

[20] Alwi N.H.M and Fan I-S. 2012. "Cultural views inclusive in e-learning risk analysis". In: 2012 IEEE Symposium on E-Learning, E-Management and E-


Services IS3e 2012, Kuala Lumpur, IEEEX plore, pp.1-6

[21] Thompson M., Ellis R. J., Ellis R. and Wildavsky. 1990. A. B., Cultural theory, Westview Pr.

[22] Karyda M., Kokolakis S. and Kiountouzis E. 2004. "Information systems security and the structuring of organisations", Proceedings of the 7th International Conference on the Social and Ethical Impacts of Information and Communication Technologies (ETHICOMP), Syros, Greece, pp. 451-461.

[23] Karyda M., Kiountouzis E. and Kokolakis S. 2005. "Information systems security policies: a contextual perspective", Computers & Security, Vol. 24, No. 3, pp. 246-260.

[24] Tsohou A., Karyda M., Kokolakis S. and Kiountouzis, E. 2006. "Formulating information systems risk management strategies through cultural theory", Information Management & Computer Security, Vol. 14, No. 3, pp. 198-217.

[25] Oltedal S., Moen B. E., Klempe H. and Rundmo T. 2004. "Explaining risk perception: An evaluation of cultural theory", Trondheim: Norwegian University of Science and Technology, Vol. 85, pp. 1-33.

[26] Mamadouh V. 1999. "Grid-group cultural theory: an introduction", GeoJournal, Vol. 47, No. 3, pp. 395-409.

[27] Alwi N. H. M. and Fan I. S. 2009. “Information security management in e-learning”. In Internet Technology and Secured Transactions. ICITST 2009. IEEE, pp. 1-6.

[28] Alwi N. H. M. and Fan I. S. 2010. “Information security threats analysis for e-learning”. In Technology Enhanced Learning. Quality of Teaching and Educational Reform, Springer Berlin Heidelberg. pp. 285-291.

[29] Albrechtsen E. 2007. "A qualitative study of users' view on information security", Computers & Security, Vol. 26, No. 4, pp. 276-289

[30] Alwi N. H. M. and Fan I. S. 2010. “Information Security in eLearning: A Discussion of Empirical Data on Information Security and eLearning”, In Proceedings of the 5th International Conference On eLearning, Academic Conferences Limited, July, p. 282.