Journal of Theoretical and Applied Information Technology
15th March 2012. Vol. 37 No.1
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETERMINING FACTORS INFLUENCING INFORMATION SECURITY CULTURE AMONG ICT LIBRARIANS

[1]MOHD SAZILI SHAHIBI, [2]ROHANA MOHAMAD RASHID, SHAMSUL KAMAL WAN FAKEH, WAN AB KADIR WAN DOLLAH, JUWAHIR ALI
Faculty of Information Management, UniversitiTeknologiMara, Shah Alam, Selangor, MALAYSIA

E-mail: [1]mohdsazili@salam.uitm.edu.my, [2]rohana.mrashid@gmail.com

ABSTRACT

The purpose of this study is to examine information security culture among and to investigate the factors that contribute to the information security culture among ICT librarians. The study uses the quantitative research method to analyze the responses to open-ended questions by 56 ICT librarians in private colleges. An empirical study is presented of an information security culture assessment instrument, which is a questionnaire, thereby providing a valid and reliable tool that can be used by organizations (libraries) to assess the in-house level of the information security culture. The evidence suggests that principles significantly influence the information security culture among ICT librarians. The developed statements in the information security culture assessment instrument are not categorized to be answered by different audiences in an organization. This could be useful as not all employees would, for instance, be in a position to answer management and strategic questions. Practitioners should understand the factors influencing the information security culture in order to develop a good culture and at the same time to protect their information assets in organization.

Keywords: *Information Security, Information Security Culture, Organizational Culture, Corporate Culture.*

1. INTRODUCTION

The development of information and communication technology services in this 21st century has become an integral part of modern life. Today, the use of information permeates most of business and private life. The use of information is seen as the most important asset in organizations and is considered to be the critical success factor of business activities. Most organizations need to protect or ensure that the information they have is secure. As with other business assets, information requires protection to ensure that it is available and confidential, and that its integrity is preserved where necessary. Especially with the widespread use of the internet, electronic handheld devices and wireless technologies have introduced more threats to the protection of information. Threats such as data theft, fraud, fire, viruses, denial-of-service attacks and even social engineering pose serious risks to the protection of information. These threats, together with careless mistakes and employee ignorance with respect to security controls, could lead to severe financial, reputational and other damages to an organization.

Securing information resources does not as a rule generate income for an organization. Business people therefore are rarely interested in how their information resources are protected. Because of that, there are some approaches that can be used to protect the information assets and knowledge in an organization, including information security management, information system security management, information risk management and security evaluation. Typically, these approaches emphasize information security and pay less attention to knowledge security. As stated by Awad and Ghaziri[1], information has a meaning, purpose and relevance, and it is about understanding relations. Meanwhile Applehans*et al.* [2] said that knowledge is the ability to turn information and data, i.e. known facts, into effective action. Besides information management, an organization has to enable knowledge creation and, from the security point of view, this means that an organization has to secure both information and knowledge [3].

When we talk about the information security culture in a library environment, of course some

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

culture has been in practice to protect their assets. For example, the culture of librarians in performing their job with guidance from their information security policy or there may be certain librarians who do not follow the policy. This is also an example of the culture that is practiced in a library environment. Another example is the culture where work is only done when there is an order from the management.

In Ernst & Young Global Information Security Survey 2004 [4], "lack of security awareness" was named by the users as the top obstacle to information security. There is no proper enforcement of ICT security policies in organizations and minimum top management efforts. Organizations must therefore move forward and be proactive in creating an information security culture and inculcate this culture in all its employees.

There have been a lot of studies on information security culture such as the information security culture framework, tools supported management of information security culture, information security culture in small and medium enterprises, information security culture from the management perspective, etc. However, there has been no direct study on the factors influencing information security culture, although these have been discussed indirectly. So this study proposes to investigate the factors influencing the information security culture especially among IT librarians in private colleges. A theoretical framework on the factors influencing information security culture was developed and hypotheses were constructed in order to test the framework.

2. INFORMATION SECURITY CULTURE

When the terms 'information security' and 'culture' are combined into a unified concept, several definitions emerge. Culture, when it comes to security, includes the beliefs, values or behavior with regard to security, or the behavior in protecting the information assets of an organization. Many researchers have come out with a definition for information security culture. The Information Security Forum (ISF) provides a comprehensive definition for an information security culture and they define it as the shared values and beliefs that people in an organization have about security [5]. They also relate information security culture to industrial safety in an organization, where the safety culture is measured by the number of incidents that occur. They argue that information security incidents in an organization occur as a result of a series of events that compromise the integrity, availability, and confidentiality of information. These events relate to the behavior of employees or their interactions with information and systems. The behavior of employees is influenced by their values and beliefs with regard to information security on the one hand and by the organization's policies on the other hand. As such, the behavior of employees and the number of incidents that occur in the organization will portray the information security culture of the organization. To summarize, the ISF definition focuses on the interaction between employees and the organization's information assets, resulting in certain behavior and incidents.

Schlienger and Teufal[6] defined information security culture by using the definition of corporate culture as earlier defined by Schein. They linked information security culture to corporate culture, where employees have certain beliefs about information security, such as "employees are our security assets". The collective values, norms and knowledge could be illustrated by every employee having to behave in accordance with the organization's information security requirements. Artifacts and creations could relate to employees annually signing off an information security policy acknowledgement statement. However Schlienger and Teufel's [7] definition is the only definition that focuses on artefacts. Although behavior is not specifically mentioned as part of the definition, the researchers refer to it when assessing the information security culture. Incidents are also not referred to specifically in the definition. However, they could fall under artifacts as a visible output of the information security culture.

Schein [8] defined corporate culture as the total of all the shared, taken-for-granted assumptions that a group has learned over time. Also, he emphasized that the core substances of corporate culture are the basic assumptions, attitudes and beliefs of employees which relate to the nature of people, their behavior and beliefs. Assumptions are values that have become embedded and, as such, are almost taken for granted. Schein[9] again mentioned organizational or corporate culture is expressed in the collective values, norms and knowledge of organizations. Values relate to the sense that people have of how things ought to be. Many values are adopted consciously and guide the actions of employees. Such norms and values affect

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the behavior of employees and are expressed in the form of artefacts and creations. Artefacts are the visible output of a culture, for example the written or spoken language or the way status is demonstrated.

Information security culture is defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics, such as integrity, confidentiality and the availability of information as the way in which things are done in an organization [10]. They also relate it to the assumption about what behavior is regarded as acceptable in protecting information and what is not. The concept of information security culture further extends to the type of behavior that is encouraged to protect information and which is not. The researchers' emphasis is on the behavior that is present as a result of the attitudes and values of the employees, since such behavior leads to the development of an information security culture. In another paper, they outlined an information security culture model consisting of organizational, group and individual levels to evaluate the information security culture in an organization [10].

The definition does not address corporate culture, which Schlienger and Teufel incorporated [8]. One could argue that the assumption about what is acceptable and what is not could relate to the attitudes, assumptions and values defined by Schein [7]. Similarly, the set of characteristics valued by the organization could relate to the values and knowledge defined by Schein.

It is important for an organization to have an information security culture. This is because when the organization has its own culture, especially in the matter of security, the organization's assets, such as information and knowledge, will be secured. Their work conduct should will automatically and naturally take security into consideration. Many recent studies have shown that the establishment of an information security culture in an organization is in fact necessary for effective information security. However, such a culture must be supported by adequate knowledge regarding information security [11]. Without adequate knowledge, users who want to behave securely might still apply a security control incorrectly. Conversely, a user who has adequate knowledge, but believes that secure behavior is unnecessary in his/her specific role, might still behave in an insecure way.

3. THEORETICAL FRAMEWORK

The theoretical framework is developed by analyzing previous research regarding information security culture. From previous research, there are four factors found based on the researchers' understanding of information security culture. The four factors are as follows:

- ***Principles***: Principles refer to the fundamental truth or proposition that serves as the foundation for a system of belief or behavior [12]. In the information security context, the principles refer to the fundamentals of information security culture, in other words what is required or should be considered when cultivating an information security culture. An example of a principle in information security is the compiling and implementing of an information security policy. According to Whitman and Mattord [13], the objective of a policy is to influence the decisions, actions and behavior of employees**.** By having principles, such as an information security policy, standards, procedures and best practices, an employee will follow all these rules and regulations and at the same time they will influence the behavior of the employee.

- ***Organizational behavior tiers***: This criterion relates to the three organizational behavior tiers defined by Robbins, Odendaal and Roodt[14] which are as follows:
  - The organizational- formal structures in the organization e.g. hierarchical or flat structure
  - Group- Employees as members of a group in an organization
  - Individual- Individuals with their characteristics e.g. age.

  All these three organizational behavior tiers develop the information security culture in the organization.

- ***Culture levels***: Schein [9] defined three levels of organizational culture, namely artefacts, values and assumptions.
  - Artefacts: Artefacts are what you can observe, see, hear, and feel in an organization. Artefacts would include visible organizational structures and processes. At the

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

level of artefacts, the culture is very clear and has an immediate emotional impact, which could be positive or negative, on the observer. Observing the artefacts alone, however, does not explain why the members of the organization behave as they do. In order to understand the reasons for the behavior patterns of organization members it is necessary to examine the "deeper" levels of a culture, such as the organization's espoused values. An easier way of understanding would be of an artefact as a visible output, such as technology [9].

- Values: An organization's espoused values are the "reasons" an organizational insider would give for the observed artefacts; for example, that the organization believes in teamwork, that everyone in the organization's view is important in the decision-making process, etc. Espoused values generally consist of the organization's official viewpoints, such as its mission- or vision-statements, strategy documents, and any other documents that describe the organization's values, principles, ethics, and vision. The espoused values are the values which the organization wants to live up to. The interpretation and application of these espoused values in the day-to-day running of the organization depends on the shared tacit assumptions between the employees of that organization [9].
- Assumptions: Often these assumptions are formed in the organization's early years because certain strategies have proven to be successful. If strategies based on specific beliefs and values continue to be successful, these beliefs and values gradually come to be shared and taken for granted. The beliefs and values become tacit assumptions about the nature of the world and how to succeed in it. These values, beliefs and assumptions that have become shared and taken for granted in an organization, form the essence of that organization's culture. Beliefs, in this sense, refer to a group of people's convictions about the world and how it works, whilst values refer to a community's basic assumptions about what ideals are worth pursuing. It is important to remember that the shared tacit assumptions resulted from a joint learning process.

- ***Security Controls***: Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks. There are many ways to minimize security risks, such as risk assessment, educating the user regarding information security (training and education, awareness campaigns, etc.). Policies and standards can also be used to control security problems. According to Chang *et al.*, [15] an acceptable level of information security can only be introduced and maintained if the correct set of security controls is identified, implemented and maintained. Identifying a reasonably effective set of security controls can be a very complicated and resource-intensive process, requiring special resources and expertise which most companies do not possess. Therefore, there exists an urgent demand for ISM standards which offer guidelines to organizations by identifying and introducing a set of controls conducive to an acceptable level of information resource protection. Ruighaver*et al.*, [16] emphasize that while employees need to learn that security controls are necessary and useful, to discourage them from attempting to bypass these controls the motivation should not just be aimed at ensuring that an employee's behavior is not compromising IS security.

Journal of Theoretical and Applied Information Technology
15th March 2012. Vol. 37 No.1
© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

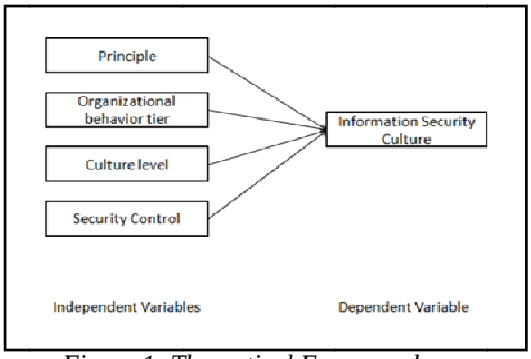

Figure 1: Theoretical Framework

4. RESEARCH METHODOLOGY

The study used the quantitative research method to analyze responses to open-ended questions. An empirical study was presented of an information security culture assessment instrument, which was a questionnaire, thereby providing a valid and reliable tool that can be used by organizations (libraries) to assess the in-house level of information security culture.

According to Belli [17], quantitative research can be divided into two general categories, which are experimental and non-experimental. For this research, the researcher used experimental research as data collection method to provide strong evidence for a cause-and-effect relationship. This is done by demonstrating that manipulation of at least one independent variable (IV) produces different outcomes in another variable, called the dependent variable (DV).

The area of the target population in this research is within the district of Petaling included Shah Alam, Petaling Jaya, Subang Jaya and Damansara. The target population was 60 ICT librarians in private college, but due to unavoidable circumstances, only 56 respondents answered the questionnaires. The SPSS (Statistical Package for the Social Sciences) was used to analyze the data from the questionnaire. The data was analyzed by using frequencies, percentages and rank orders. Pearson's Correlation was also used to test hypothesis.

5. FINDINGS AND DISCUSSION

In an effort to investigate the factors influencing information security culture, i.e. the principles, organizational behavior tier, culture levels and security controls, a correlation analysis was performed. Consequently, a bivariate correlation analysis was separately executed between each of the abovementioned variables and the information security culture. The results of the correlation analysis between the factors influencing the information security culture are displayed in Table 1. The value of Pearson's 'r' range from r = 0.100 to r = 1.472, suggests that a positive correlation and substantial relationship exists. The lowest correlation value r = 0.185 is between the culture level and the information security culture, and the highest correlation is between the principle and the information security culture.

Table 1: Correlation Analysis between Factor and Information Security Culture

Factor	Information Security Culture
Principle	0.472**
Organizational Behavior Tier	0.248
Culture Level	0.185
Security Control	0.322*

**. Correlation is significant at the 0.01 level (2-tailed).

Principle as a Factor Influencing Information Security Culture

To investigate whether principle is one of the factors influencing the information security culture, the following hypothesis was developed:

- *H1: Principles significantly influence the information security culture among ICT librarians in private colleges.*

Pearson's correlation analysis method was used to determine whether principles influence the information security culture. As shown in Table 2, principle was found to have a moderate correlation and substantial relationship with the information security culture (r = 0.472). The 'p' value which is (0.000) shows that there is a significant difference between principle and information security culture because $p<0.05$. Based on this finding, the formulated hypothesis, *H1: Principles significantly influence the information security culture among IT librarians in private colleges*, is therefore accepted.

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Principle Correlation

		Information Security Culture (ISC)	Principle
ISC	Pearson Correlation	1	.472**s
	Sig. (2-tailed)	0	.000
	N	56	56
Principle	Pearson Correlation	.472**	1
	Sig. (2-tailed)	.000	
	N	56	56

Organizational Behavior Tier as a Factor Influencing Information Security Culture

In order to examine whether the organizational behavior tier influences the information security culture, the following hypothesis was formulated:

- *H2: The organizational behavior tier significantly influences the information security culture among IT librarians in private colleges.*

As shown in Table 3, the OBT (organizational behavior tier) indicates the value of Pearson's correlation, r = 0.248. This value presents a low correlation and weak relationship between the organizational behavior tier and the information security culture. The 'p' value, which is more then 0.05 (p = 0.065), shows that there is no significant difference. Based on this finding, the formulated hypothesis, *H2: The organizational behavior tier significantly influences the information security culture among IT librarians in private colleges,* is therefore not accepted.

Table 3: Organizational Behavior Tier Correlation (OBT)

		Information Security Culture (ISC)	OBT
ISC	Pearson Correlation	1	.248
	Sig. (2-tailed)	0	.065
	N	56	56
OBT	Pearson Correlation	.248	1
	Sig. (2-tailed)	.065	
	N	56	56

Culture Level as a Factor Influencing Information Security Culture

The study on culture level as a factor influencing information security culture revealed the following hypothesis:

- *H3: The culture level significantly influences the information security culture among IT librarians in private colleges.*

Based on Table 4, the probability value, which is more than the significant level (p = 0.173, p > 0.05), shows that there is no significant difference between the culture level and the information security culture. The 'r' value, which is 0.185, shows that there is a slight correlation and a relationship that is so small as to be negligible. Based on this finding, the formulated hypothesis, *H3: The culture level significantly influences the information security culture among IT librarians in private colleges,* is therefore not accepted.

Table 4: Culture Level Correlation

		Information Security Culture (ISC)	Culture Level
ISC	Pearson Correlation	1	.185
	Sig. (2-tailed)	0	.173
	N	56	56
Culture Level	Pearson Correlation	.185	1
	Sig. (2-tailed)	.173	0
	N	56	56

Security Control as a Factor Influencing Information Security Culture

To investigate whether security control influences the information security culture, the following hypothesis was developed:

- *H4: Security control significantly influences the information security culture among ICT librarians in private colleges.*

Table 5 shows the security control correlation. The 'r' value, which is 0.322, shows that there is a low correlation and weak relationship between the

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security control and the information security culture. The 'p' value, which is 0.016 ($p > 0.05$), shows that there is no significant difference between the two variables. Based on this finding, the formulated hypothesis, H4: *Security control significantly influences the information security culture among ICT librarians in private colleges*, is therefore not accepted.

Table 5: Security Control Correlation

		Information Security Culture (ISC)	Security Control
ISC	Pearson Correlation	1	.322*
	Sig. (2-tailed)		.016
	N	56	56
Security Control	Pearson Correlation	.322*	1
	Sig. (2-tailed)	.016	
	N	56	56

6. LIMITATION AND FUTURE RESEARCH DIRECTIONS

The current research study has the following limitations:

- Research method: This study only implicates the quantitative research method where information is gathered purely through questionnaire. Qualitative research method such as interview can be used and tested for future research.

- Assessment data: The information security culture assessment data used to validate the assessment instrument are obtained from one profession only which is IT librarian. The research study does not incorporate more than one surveys data nor does it extend to a second survey in the same organization. Further research can be conducted to enable researcher to benchmark the data and identify whether the information security culture indeed improved after the implementation of action plans.

- Assessment instrument: The developed statements in the information security culture assessment instrument are not categorized to be answered by different audiences in an organization. This could be useful as not all employees would for instance be in the position to answer the management and strategic questions. For future research, researcher may conducted the research and categorized the assessment instrument according to the level of management or only focus to the top level management to investigate the information security culture problem.

- Design of assessment instrument: The design of assessment instrument used in the study are not designed in appropriate way for example researcher used three likert scale to measure the level of agreement of respondent which is inappropriate. The five or seven or more likert scale is better to measure the level of agreement.

7. CONCLUSION

The research discovered that principles are most significant factor influence Information Security Culture. After conducting the correlation analysis test to examine the factors influencing the information security culture, this section aims to provide an overview of the results of the study. The results of the study show that an only principle is strongest factor, significantly influences the information security culture. Figure 2 below illustrates the study according to the strength of the relationship adopted from Pearson's correlation analysis.

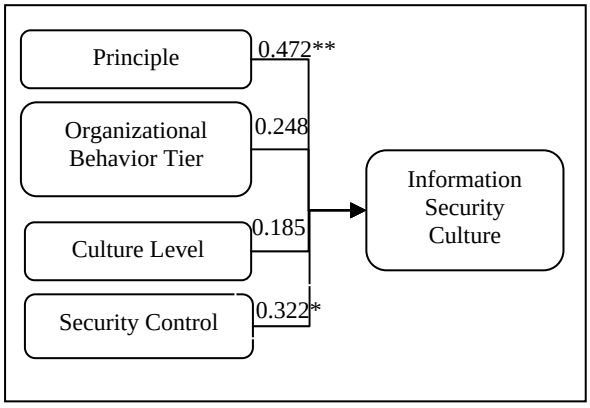

Figure 1: Result of the Study

According to Zakaria [18], organizations could use the principles of information security as a stepping stone in developing the information security culture among employees. Identifying the information security culture challenges in the

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organization can be the first step in developing such information security culture. The participation and cooperation from all employees are the best ways for establishing a good information security culture. This can in turn create a good security culture environment in the library or any organization. Besides, it will minimize the risk of internal security incident.

REFRENCES:

[1] Awad, E., & Ghaziri, H. (2003). *Knowledge Management.* Prentice Hall.

[2] Applehans, W., Globe, A., & Laugero, G. (1999). *Managing Knowledge* . Boston MA: Addison Wesley.

[3] Krogh, G., Ichijo, K., & Nonaka, I. (2000). *Enabling knowledge creation: How to unlock the mystery of tacit knowledge and release the power of innovation* . Oxford University Press.

[4] Ernst & Young (2004), Global Information Security Survey 2004, Retrieved from http://www2.eycom.ch/publications/items/saas_global_security_survey_2004/en.pdf

[5] Information Security Forum, Information (2000), Security Culture- A Prelimenary investigation s.l.

[6] Schlienger, T., & Teufel, S. (2005). Tools supported management of information security culture. . *IFIP International Information Security Conference (20th:*

[7] Schlienger, T., & Teufel, S. (2002). Information Security Culture. *Security in the Information Society. IFIP/SEC2002* (pp. 191-201). Boston: Kluwer Academic Publishers.

[8] Schein, E. H. (1999). *The Corporate Culture* . United States of Americe: Jossey-Bass Publishers.

[9] Schein, E. H. (2004). *Organizational culture and leadership* (3rd edition ed.). San Francisco: The Jossey-Bass.

[10] Martin, A., & Eloff, J. (2003). Information Security Culture, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002). *IFIP Conference Proceedings 214*, (pp. 203-214). Cairo, Egypt.

[11] Niekerk, J. V., & Solms, R. V. (2005). An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security South Africa (ISSA)* .

[12] Oxford Dictionary, (2010)

[13] Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security, Second Edition.* Australia: Thomson Course Technology.

[14] Robbins, S.P., Odendaal, A. and Roodt, G. (2003). Organizational Behavior: Global and Southern African perspectives. Cape Town: Pearson Education South Africa.

[15] Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Managemnet and Data Systems, 107* (3), 438-458.

[16] Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security* , 56-62.

[17] Belli, L. F. (2004). Reading and understanding research. Information Systems Research 15 ,34.

[18] Zakaria, O. (2007). *Investigating information security culture challenges in a public sector organization: a Malaysian case.* Royal Holloway, University of London.

© 2005 - 2012 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTHOR PROFILES:

Mohd Sazili Shahibi is Director of Malay Thought and Leadership Institute,UniversitiTeknologi Mara (UiTM) and Senior Lecture in Faculty of Information Management UiTM, ShahAlam, Selangor, Malaysia. He obtained PhD in area of Information System Management from University of Malaya, Kuala Lumpur.

RohanaMohamad Rashid received the Bachelor of Scienceand Master of Sciencein Information Management from UniversitiTeknologi Mara. Currently, she is a PhD student in UniversitiPertahananNasional Malaysia and doing the PhD in Computer Science and Technology.

Shamsul Kamal Wan Fakehreceived Master of Science in Information Management from UniversitiTeknologi Mara. Currently he isSenior Lecturer in Faculty of Information Management,UniversitiTeknologi Mara, ShahAlam. Selangor, Malaysia.

JuwahirAli received the Master of Science in Information Technology from East London University, UK. Currently he isSenior Lecturer in Faculty of Information Management,UniversitiTeknologi Mara, Shah Alam, Selangor, Malaysia.

Wan AbKadir Wan Dollah Head of Library Science and Information ResourcesDepartment andSenior Lecturerin Faculty of Information Management, UniversitiTeknologi Mara, Shah Alam, Selangor, Malaysia. He received PhD in area of Library and Information Science from University of Malaya Kuala Lumpur.