Users' Perception on the Information Security Policy of the Institutions of Higher Learning

Haniza Sharif[a], Zuraini Ismail[b], Maslin Masrom[c]

[a]Center For Advanced Software Engineering
Universiti Teknologi Malaysia, International Campus, Jalan Semarak, 54100 Kuala Lumpur
Tel : 013-3620836, Fax : 03-22748352
E-mail : honez@bnm.gov.my, honez2007@yahoo.com.my

[b]College of Science and Technology
Universiti Teknologi Malaysia, International Campus, Jalan Semarak, 54100 Kuala Lumpur
Tel : 03-26154778, Fax : 03-26154315
E-mail : zurainisma@citycampus.utm.my

[c]College of Science and Technology
Universiti Teknologi Malaysia, International Campus, Jalan Semarak, 54100 Kuala Lumpur
Tel : 03-26154672, Fax : 03-26154225
E-mail : maslin@citycampus.utm.my

ABSTRACT

Securing information is essential for safeguarding the organization business operations as information is a business asset to any organization including education sector. One of the most imperative information security (InfoSec) controls identified is InfoSec policy, a direction-giving document. The purpose of this study is to investigate the user awareness, understanding and acceptance of InfoSec policy in the Malaysian's Institutes of Higher Learning. Survey questionnaires had been distributed to graduate students and non-IT staff of Universiti Teknologi Malaysia (UTM), International Campus, Kuala Lumpur. The result of this study had perceived consistent agreeable behaviors of the InfoSec policy within UTM.

Keywords
Information security policy, Enforcement, Effectiveness, Awareness, Understanding, Acceptance

1.0 INTRODUCTION

Undoubtedly, developments in Information and Communication Technologies (ICTs) have impacted all sectors including Institutes of Higher Learning (IHL). As computer usage becomes more and more pervasive, it provides the ability for IHL to automate, adapt and accelerate their learning strategy. Similarly, ICTs provides great opportunity for IHL to improve their business strategic operations.

The modern world thrives on information and its flows; the contemporary world, society, and institutions cannot function without their computer-communication-based information system (Pfleeger & Pfleeger, 2007). The effect from this situation had exposed the information system to probable threats and risks. Hence, these systems must be protected from all aspects; technical, procedural, operational and environmental. Thus, the institutions need to be responsible in protecting their organisation's information assets.

Some of the control measures that an institution can adopt are well-documented policy, installation of firewall or latest antivirus, or the implementation of a biometric system for physically control access. Despite these measures, lack of management support, and lapses on enforcement, awareness, understanding and acceptance of the organisation's information security (InfoSec) policy might weaken the existing security arrangements.

An investigation to examine the status of the InfoSec policy enforcement and its effectiveness from the users' perspective of awareness, understanding and acceptance particularly in the Malaysian's IHL environment are needed. It is also timely, primarily due to the lack of study conducted in this area. In this paper we will investigate the status of the InfoSec policy enforcement and the effectiveness from the user's perspective within the Universiti Teknologi Malaysia (UTM) environment.

This paper is organized into five sections. This section enlightens the impact of ICTs to various sector including IHL and scope of this study. A review of literature is explained in section two while section three describes the methodology and approach adopted in conducting this study. The findings are available in section four. Section five provides the discussions and conclusions of the study.

2.0 LITERATURE REVIEW

This section reviews the literature on InfoSec policy definition and framework.

2.1. Information Security Policy Definition

Information is an asset. Having specific and relevant information can make a massive difference to an organization's efficiency. With a huge number of available technologies, it is possible for information to be collected, shared, sold, exchanged and distributed without citation or notice to the owner (Varmey, 1996).

InfoSec involves the protection of information with the aim the information system can deliver the highest security as possible through (i) confidentiality by ensuring only those with legitimate right can access it, (ii) integrity for protecting the information from being maliciously or intentionally changed, and (iii) availability by making information available when and where needed by authorized person (Hone & Eloff, 2002).

A policy on the other hand, is a formal, brief, and high-level statement that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area (Sandy, 2008).

Other definition states that policy is typically a document that outlines specific requirements or rules and can be thought as an equivalent of institution specific law that must be met by institution (The SANS™, 2008). Thus, InfoSec policies must be carefully crafted to reflect a mission and objectives of the organization. Without this synergy, the policy will never succeed (DesPlanques, 2005).

Security policies are the foundation and the bottom line of information security in any organization. A well written and implemented policy contains sufficient information on what must be done to protect information and people in the organization (Kee, 2001).

To summarized, the InfoSec policy is a plan identifying the organization's vital assets together with a detailed explanation of what is acceptable, unacceptable and reasonable behavior from the employee in order to ensure security of information.

2.2. Information Security Framework

In general, framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. From the InfoSec policy perspective, a framework offers a possible starting point for understanding a security policy's impact to an organization, and is intended to guide organizations in developing, implementing, and maintaining security policy (Rees et al., 2003).

From the literature review revealed that different organizations adopted different InfoSec policy framework model although the organizations are within the same sector. The reason being that as the threats to information assets are varied depending on the organization's environment. Moreover, an adequate security level for one IT system or business process may be insufficient for another due to different organization's size, complexity, and culture. Thus, the InfoSec policies framework is most effective when it is map and developed based on organization's specific needs.

2.3. Conceptual Framework

Figure 1 depicts the research model for this study. The model presents a theoretical framework for effective InfoSec policy based on the relationships between research variables.

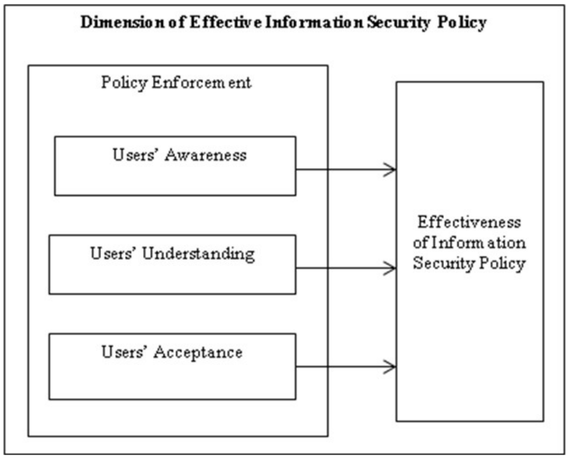

Dimension of Effective Information Security Policy
Policy Enforcement
Users' Awareness
Users' Understanding
Users' Acceptance
Effectiveness of Information Security Policy

Figure 1: The proposed Research Model

The following variables are considered in operationalizing the research model.

2.3.1. Effective Information Security Policy

InfoSec policy is a document that is understandable, meaningful, practical and also must be implementable, enforceable, realistic and usable (Hone, 2004). Most importantly, the document must speak to the users and convince them of the importance of protecting the institution's information resources.

According to Tudor (2001), InfoSec policy is a formal statement of an organization wishes to achieve with regards to the InfoSec discipline. Hone and Eloff (2002) then states that InfoSec policy is one of the most important controls needed within an organization to ensure the effectiveness of

InfoSec. Hone (2004) further states than an effective InfoSec policy assists in achieving the organisation's InfoSec objectives. Thus, effective InfoSec policy is crucial in ensuring the successfulness of the organization's business operations.

The dependent variable of this study is an effective InfoSec policy and it has been a significant justification to the InfoSec research. The successful InfoSec policy provides several benefits to corporations (Ungerman, 2005). Hone and Eloff (2002) states, "at the end of the day, an effective InfoSec policy will directly result in effective InfoSec".

This study will explore the user's perceptions on the effectiveness of InfoSec policy, and the policy enforcement and it's supporting components: awareness, understanding and the acceptance of the InfoSec policy to ensure the policy is and remains an effective InfoSec policy.

2.3.2. Policy Enforcement

Madigan et al. (2004) clarifies that policy enforcement involves assuring that the policies are understood by all interested parties, regularly checking to see if the policies are being violated, and having well-defined procedure guidelines to deal with incidents of policy violation.

Canavan (2003) explains that the InfoSec policy can only be enforced by means of implementation. When an organization puts an InfoSec policy into practice, employees can be requested to follow the rules and be made aware of their rights and responsibilities (Hone & Eloff, 2002). A security policy can mitigate some threats, such as viruses, and work towards preventing incidents caused by these threats from re-occurring (Hinde, 2003).

The variables identified for this study are as follows:

i. Users' Awareness

In determining the perceptions of user's awareness of InfoSec policy, the awareness elements are observed. The following are the basic questions raised based on previous study conducted (EDUCAUSE, 2001; Shariff N., 2007):

A. Whether the users have heard about their institution's InfoSec policy and its importance?
B. Did the users know about the requirements in their institution's InfoSec policy?
C. Whether the users knew what was expected, and familiar with the consequence and effect of complying / not complying with the policy?

ii. Users' Understanding

The InfoSec policy should be clear, precise and practical to be implemented without compromising the security. The following questions are adopted and adapted from previous study (EDUCAUSE, 2001; Shariff N., 2007):

A. Whether the users clear with the institution's aim and objectives of adopting and implementing the InfoSec policy?
B. Whether the user understood the necessary steps to secured information and the equipments?
C. Whether the users believed the important to make a report for any security incidents to the managements or authorized officer?

iii. Users' Acceptances

The InfoSec policy is a plan identifying the organization's vital assets together with an explanation of what is acceptable, unacceptable and reasonable behavior from the employee in order to ensure security of information (Hone & Eloff, 2002).

The questions posted are (EDUCAUSE, 2001; Shariff N., 2007):

A. Whether users committed about institution's InfoSec policy?
B. Whether users realized that InfoSec activities had been applied within the institution?
C. Whether users had practices the password management requirements?

The outcome from these questions will be analyzed to portray the users' perception on the enforcement and effectiveness of the InfoSec policy.

3.0 METHODOLOGY

The strategies selected for this study are based on two basic research questions:

A. What is the status of InfoSec policy implementation in the institution?
B. What is the user's perception towards the enforcement and effectiveness of the institution's InfoSec policy?

In achieving the study's objectives, research methodology of qualitative and quantitative was adopted in conducting the exploratory study.

3.1. Qualitative Method

To explore the status of InfoSec policy implementation of UTM, an interview was selected as a method of data gathering. An IT-expert staff involved in reviewing the existing IT environment and was in-charge of developing the InfoSec policy for the institution was identified.

The interview session was conducted approximately for two hours and the process was conducted in a structured manner. A set of questionnaires was prepared as a guideline in steering the interviewing process. The interview provides an overview of InfoSec policy implemented at the institution.

3.2. Quantitative Method

Survey was chosen as a data collection method for this study to seek the user's perceptions on InfoSec policy. Unit analysis of this method is graduate students and non-IT staff that uses the institution's IT facilities in executing their daily activities.

To perform the survey, the items in the questionnaires had been refined based on the previous studies (EDUCAUSE, 2004; Shariff N., 2007) conducted. A study was carried out with a total of 335 questionnaires were distributed to students and non-IT staff of UTM, *International Campus*, Kuala Lumpur.

The questionnaires are divided into five sections. Section one taps the demographic makeup of the respondents. The other sections are Users' Awareness, Users' Understanding, Users' Acceptance and Effectiveness of the InfoSec policy. For consistency, an evaluation scheme as shown in Table 1 was used in answering the questionnaires.

Table 1: *Description of Evaluation Scheme*

Evaluation Option	Score	Meaning
Not Applicable	0	When the given statement is not relevant either by the facilities provided by the Institution or the role of the user do not require such practices.
Strongly Disagree	1	The statement is **never consistent** of or not practiced at all by the user.
Disagree	2	The statement is **most of the time not consistent** of or not being practiced by the user.
Agree	3	The statement is **most of the time** reflective or being practiced by the user.
Strongly Agree	4	The statement is **consistently** holding true or being practiced by the user.

4.0 FINDINGS OF STUDY

The result from the interview is provided in section 4.1 while the findings of the survey are presented in section 4.2 and 4.3.

4.1. Establishment Of Information Security Policy In the Institution

The institution has set up an Information Technology (IT) Committee which is responsible for overseeing and ensuring smooth running of IT operations within the institution. The committee consists of the institution's IT-experts and top management. Through an interview it was found that any amendments of current or new Information, Communication and Technologies (ICTs) policy need to be submitted for approval only at the faculty level. The rational is that the policy is relevant and applies only to certain faculties or departments.

As an initiative, the institution had also set up a project team to review the status of IT environment and the implementation of the existing InfoSec policy within the institution. The objective of this team is to identify the problems with regards to IT arrangements for the institution. A report is prepared and submitted to the IT Committee in order to provide relevant proposal in enhancing the InfoSec policy for the institution.

Despite the disparity among faculties, the IT Committee had approved seven new set of ICTs policy which is more comprehensive and relevant to all level across the institution.

4.2. Demographic Profile

The study was conducted in January and February, 2009 which covered graduate students and non-IT staff of UTM, *International Campus*, Kuala Lumpur. Out of 335 questionnaires distributed 225 participants interpreted to 67 % of respond rate. Table 2 portrays the demographic profile of the respondents by gender, role within the institution and role in enforcing InfoSec policy compliance.

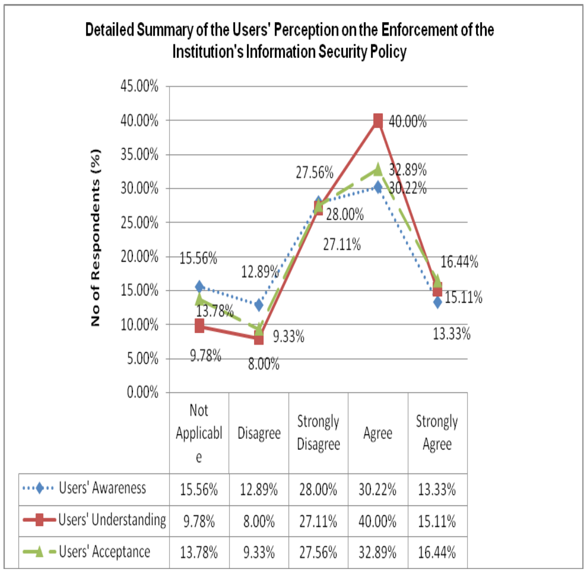
Table 2: *Demographic Profile*

	Frequency (N)	*Percentage (%)*
a. Gender		
1. Female	120	53
2. Male	105	47
b. Respondent role with Institution		
1. Student	212	94
2. Staff (non-IT)	13	6
c. Respondent role in enforcing InfoSec compliance		
1. Users	216	96
2. Some role in supervising	5	2
3. Others	4	2

4.3. User's Perception On The Enforcement And Effectiveness Of The Institution's Information Security Policy

An overview of the user's perception from the study is shown in Figure 2. The vertical axis represents the percentage of respondent while the horizontal axis reflected the three key indicators which are awareness, understanding and acceptance.

All variables are evaluated based on the standard evaluation scheme as shown in Table 1. The overall result from the responds revealed that all three key indicators for measuring the enforcement of the InfoSec policy perceived by either Agree or Strongly Agree behavior.

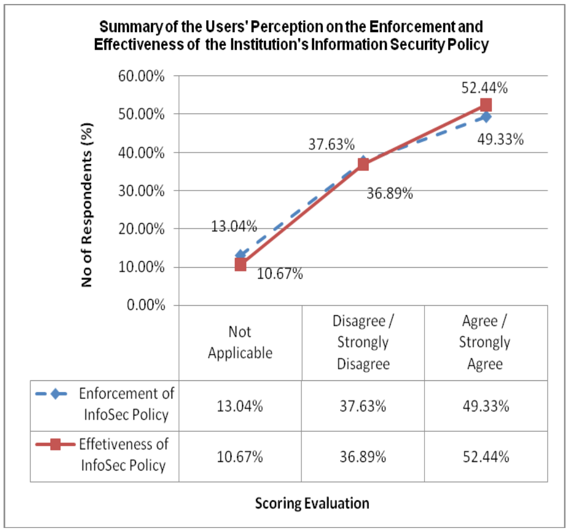


	Not Applicable	Disagree	Strongly Disagree	Agree	Strongly Agree
Users' Awareness	15.56%	12.89%	28.00%	30.22%	13.33%
Users' Understanding	9.78%	8.00%	27.11%	40.00%	15.11%
Users' Acceptance	13.78%	9.33%	27.56%	32.89%	16.44%

Figure 2: Detailed Summary Of the Users' Perception On The Enforcement of the Institution'sInformation Security Policy

The figure shows that less than half (43.55% and 49.33%) of the respondents is generally aware and accepts the institution's InfoSec policy.

On the other hand, the perception of the users' understanding on the enforcement of the InfoSec policy portrayed more than half (55.11%) of the respondents had rated 'Strongly Agree' and 'Agree' to the survey.



	Not Applicable	Disagree / Strongly Disagree	Agree / Strongly Agree
Enforcement of InfoSec Policy	13.04%	37.63%	49.33%
Effetiveness of InfoSec Policy	10.67%	36.89%	52.44%

Figure 3: Summary Of the User's Perception On The Enforcement And Effectiveness Of The Institution's Information Security Policy

As depicts in Figure 3, the overall analysis from the study on the enforcement and effectiveness of the institution's InfoSec policy from the users' perspective revealed that nearly half (49.33%) of the respondents agreed that the policy had been properly enforced within the institution, whereas more than half (52.44%) indicated that the policy is effective.

5.0 DISCUSSIONS AND CONCLUSIONS

The first stage of the study which is based on interview has established the existence and the important of the InfoSec policy within the institution. The institution has taken necessary steps of setting up a project team in order to review and provide advice to IT Committee and developing a relevant proposal on ICTs policy in order to enhance the IT security of the institution.

However, from the study conducted which focusing on enforcement and effectiveness of established InfoSec policy reveals that nearly half of the respondents perceived that the policy had been enforced and it is found to be effective. Thus, this still indicates that more concern is requires for the implementation of InfoSec.

Therefore, the institution should further improve their security control by enhancing the operating procedure towards the effectiveness of the policy. Besides, the institution can also create awareness amongst the students and staff by incorporating the need to secure the computer and information as part of the institutions' activities and program.

Nevertheless, this study provides some indication to the institution on their security level which probably requires more attention to further enhance the security control within the institution. The study also had proposed a theoretical framework and the potential variables that can be considered to signify the effectiveness of the InfoSec policy for the institution. Even though this study does not test or validate any hypothesis or relations amongst the variables, the proposed framework may be useful as a basis for reference not only for researchers in this field but also for practitioner in developing the InfoSec policy.

This study covered only one institution as the unit of analysis. Thus, in order to gain more fair and accurate findings, it is recommended that the future research should include more Institutions of Higher Learning particularly in the Malaysian context.

REFERENCES

Canavan, S. (2003). An Information Security Policy Development Guide for Large Companies. *The SANS™ Institute, 2001.*

DesPlanques, D. (2005). Information Security Policy Development for Institutions of Higher Education. *Thesis for Master. Regis University, School for Professional Studies*. 2005.

EDUCAUSE; Security Tasks Force (2004). Information Security Governance Assessment Tool For Higher Education. Boulder, Colorado and Washington, D.C. *EDUCAUSE.*

Hinde, S. (2002). Security Surveys Spring Crop. *Computers and Security*, Vol. 21, No. 4, pp. 310-321.

Hone, K., & Eloff, J.H.P. (2002). What makes an Effective Information Security Policy. *Network Security*, Vol. 20, No. 6, pp. 14-16.

Hone, K. (2004). The Information Security Policy – An Important Information Security Management Control. (Degree Dessertation, Rank Afrikaans University, 2004). *Dessertation of Mcom (Informatic), Faculty of Economic and Management Science.*

Kee, C.K. (2001). Security Policy Roadmap – Process for Creating Security Policies. *The SANS™ Institute, 2001.*

Madigan, E. M., Petrulich, C., & Motuk, K. (2004). The cost of Non-Compliance - When Policies Fail. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, pp. 47 – 51, USA.

Pfleeger, C.P., & Pfleeger, S.L. (2007). *Security in Computing.* (4th ed): Pearson Education, Inc (Pearson International Edition).

Rees, J., Bandyopadhyay, S., & Spafford. E. H. (2003). A policy framework for information security. *CERIAS Tech Report 2003-35, July 200 3, Vol. 46, No. 7 Communications of the ACM.*

Shariff, N. (2007). Conceptualizing and Developing Information Security Awareness and Training Programme, Case Study: Malaysian Financial Sector. (Master dissertation, Centre for Advanced Software Engineering, Universiti Teknologi Malaysia *International Campus*, Kuala Lumpur) *Dissertation for Master (Information Security),* CASE, Faculty of Computer Science and Information, System, UTM.

The SANS™; No author (2008). IT Security Policies. *The SANS Institute* 8120 Woodmont Avenue, Suite 205 Bethesda, Maryland. Retrieved September 20, 2008, from http://www.sans.org/resources/policies.

Tudor, J. K. (2001). Information Security Architecture: An Integrated Approach to Security in the Organization. *CRC Press LLC*. ISBN 0-8493-9988-2.

Ungerman, M. (2005). Creating and Enforcing an Effective Information Security Policy. *Information Systems Control Journal*, volume 6, ISACA®, Inc.

Varney, C. A. (1996). Consumer Privacy in the Information Age: A View from the United States. *Remarks before the Privacy and American Business National Conference, Washington.*