Chapter 21
ICT Security Policy in a Higher Education Institution in Malaysia

Fardzah Sulaiman
University Sains Malaysia, Malaysia

T. Ramayah
University Sains Malaysia, Malaysia

Azizah Omar
University Sains Malaysia, Malaysia

ABSTRACT

Information and **c***ommunication technology (ICT) is an important strategic and essential functional requirement for many institutions of higher learning. In the developing world, ICT is achieving breakthrough in management and teaching through online learning, which helps to cater for the increasing student population. However, the security of the information being processed stored and exchanged is a growing concern to the management as the dependence on ICT for most of the institutions' core services functions are increasing. This chapter discusses the current state of ICT security policy practices in University Science of Malaysia (USM); one of the Higher Education Institution in Malaysia. USM has been granted accelerated programme for excellence (APEX) status due to the mission of readiness, transformation plan and preparedness to change and transform it into Malaysia's first world-class university. The discussion encapsulates the problems, consequences of ICT risks and ICT awareness. Furthermore, it highlights the ICT policy guideline, ICT security policy formulation, ICT security management safeguards, principles and ICT security and adherence compliance plan.*

INTRODUCTION

The internet-driven global digital revolution and the explosive growth of computer networks and systems have resulted in the extensive use of information and communications technology (ICT) in higher education institutions (HEIs) in Malaysia. Electronic connectivity - for gathering, maintaining and transmitting information and data in the work place has meant that the security of ICT systems and information residing in them can no longer be provided through conventional means. The increasing incidence of hacking, virus attacks and other forms of electronic trespass

DOI: 10.4018/978-1-61520-847-0.ch021

have necessitated the need for securing the new electronic work environment. The HEI is not insulated from the prevailing dangers of the digital world. For that matter, considering the scope of its functions, services and transactions as well as the complexities of its inter-relationships with all components of society, the HEI has to seriously address all concerns relating to ICT security.

ICT security is critical to the objectives of implementing and expanding the use of ICT in the delivery of services as well as in enhancing the internal operations of public HEI. In this regard, the government of Malaysia has already issued a broad policy guideline on the underlying principles of ICT security, the responsibility of safeguarding government information and the need for awareness about threats to the integrity of information and ICT assets. In addition, guidelines on the mechanism for reporting ICT security incidents were also issued to assists agencies in handling ICT security incidents in HEI. The Malaysia Public Sector ICT Management Security Handbook (MyMIS) is intended as a reference and guide for public sector personnel in managing security in all public sector ICT installations (MyMis, 2002).

MyMIS handbook is the product of Malaysian Administrative Modernization and Management Planning Unit (MAMPU), where one of MAMPU functions is to plan administrative modernisation and human resources in Malaysia.

ICT SECURITY

ICT security can be defined as "the process of ensuring business continuity and services provision free from unacceptable risk. It also seek to minimize disruptions or damage by preventing and minimizing security incidents" – report from Public Sector ICT Security Policy (2000) pp 1.

The purpose of ICT security policy is to help the stakeholder to provide effective and efficient services and to ensure that all users of the ICT systems aware of the security risks that are always present such as threats whether internal or external, deliberate or accidental. ICT security policy in HEI will contain standards for information security, comprehensive sets of security controls to improve the level of security within the organisation. In addition to this policy, a wide-ranging set of standards, procedures and protocols governing the use of the ICT is available on the Intranet.

The Government of Malaysia is committed towards modernising its administrative machinery and enhancing its service delivery mechanisms. The process of ensuring an efficient and effective public sector is being driven by the enabling capabilities of information and communication technology (ICT). The resultant widespread adoption of ICT systems by the public sector has meant that more and more government agencies are moving towards the paperless work environment where ICT systems have become indispensable for the provision of government services to citizens.

The tremendous increasing numbers of public institutions of higher learning (IPTA) and private institutions of higher learning (IPTS) in Malaysia show the need of ICT systems and security. The expansion of ICT systems within the HEI has in turn led to a significant increase in the number of public information repositories and other ICT-based installations and assets. The security of these ICT installations and assets are exposed to the vulnerability due to the dependency and usage especially with the advent of the Internet, exposes HEI information to a much larger audience and with that a potential threat that HEI information being compromised. This is especially worrying on classified HEI information and if left unchecked, can cause serious integrity issues. At the same time, there need to be a balance between rigid information control that limits service delivery on one hand against a loose information control that would compromise security or severely affect the interest of the public service or the nation.

The Cardinal ICT Security Principles (Table 1) protects against loss of Confidentiality, Integrity, Available, Authenticity and Non repudiation